Nos. 2024-1278, 2024-1354

United States Court of Appeals for the Federal Circuit

CPC PATENT TECHNOLOGIES PTY, LTD.,
Appellant

v.

APPLE, INC.,
Appellee

Appeals from the United States Patent and Trademark Office,
Patent Trial and Appeal Board in Nos. IPR2022-00601, IPR2022-00602

CORRECTED BRIEF OF APPELLANT CPC PATENT TECHNOLOGIES PTY, LTD.

K&L GATES LLP

GEORGE C. SUMMERFIELD
JONAH B. HEEMSTRA
70 W. Madison Street, Suite 3300
Chicago, IL 60602
(312) 372-1121
george.summerfield@klgates.com

DARLENE F. GHAVIMI-ALAGHA
2801 Via Fortuna, Suite 650
Austin, Texas 78746
(512) 482-6800

Attorneys for Appellant

April 23, 2024

CHALLENGED CLAIMS OF THE '208 PATENT

[1pre] A system for providing secure access to a controlled item, the system comprising:

[1a] a database of biometric signatures;

[1b] a transmitter sub-system comprising:

[1b1] a biometric sensor for receiving a biometric signal;

[1b2] means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

[1b3] means for emitting a secure access signal conveying information dependent upon said accessibility attribute; and

[1c] a receiver sub-system comprising:

[1c1] means for receiving the transmitted secure access signal; and

[1c2] means for providing conditional access to the controlled item dependent upon said information,

[1d] wherein the transmitter sub-system further comprises means for populating the data base of biometric signatures, the population means comprising:

[1d1] means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

[1d2] means for mapping said series into an instruction; and

[1d3] means for populating the data base according to the instruction,

[1e] wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

[3a] The system according to claim 1, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class,

[3b] the accessibility attribute preferably comprising: an access attribute if the biometric signal matches a member of the database of biometric signatures;

[3c] a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

[3d] an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

[4] The system according to claim 1, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration, and/or the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

[5] The system according to claim 1, wherein said conditional access comprises one of:

provision of access to the controlled item if the accessibility attribute comprises an access attribute:

provision of access to the controlled item and sounding of an alert if the accessibility attribute comprises a duress attribute; and

denial of access to the controlled item and sounding of an alert if the accessibility attribute comprises an alert attribute.

[6a] The system as claimed in claim 1, wherein: the biometric sensor is for authenticating the identity of a user;

[6b] the means for emitting comprises a transmitter for transmitting information capable of granting more than two types of access to the controlled item using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and

[6c] the system further comprising a control panel for receiving the information and for providing the secure access requested.

[7] The system according to claim 6, wherein the control panel includes a converter for receiving the secure wireless signal and for outputting the information, and/or the biometric sensor authenticates the identity of the user by comparing a biometric input from the user with a biometric signature for the user in a biometric database, and/or the biometric sensor, the biometric database, and the transmitter are located in a remote fob.

[9pre] A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:

[9a] a biometric sensor for receiving a biometric signal;

[9b] means for matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and

[9c] means for emitting a secure access signal conveying said information dependent upon said accessibility attribute;

[9d] wherein the transmitter sub-system further comprises means for populating the database of biometric signatures, the populating means comprising:

[9d1] means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

[9d2] means for mapping said series into an instruction; and

[9d3] means for populating the database according to the instruction,

[9e] wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

[10pre1] A method for providing secure access to a controlled item in a system comprising

[10pre2] a database of biometric signatures,

[10pre3] a transmitter sub-system comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal capable of granting more than two types of access to the controlled item, and

[10pre4] a receiver sub-system comprising means for receiving the transmitted secure access signal, and

[10pre5] means for providing conditional access to the controlled item dependent upon information in said secure access signal,

[10a] the method comprising the steps of: populating the database of biometric signatures by:

[10a1] receiving a series of entries of the biometric signal;

[10a2] determining at least one of the number of said entries and a duration of each said entry;

[10a3] mapping said series into an instruction; and

[10a4] populating the database according to the instruction;

[10b] receiving a biometric signal;

[10c] matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;

[10d] emitting a secure access signal conveying information dependent upon said accessibility attribute; and

[10e] providing conditional access to the controlled item dependent upon said information,

[10f] wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

[11] The method according to claim 10, wherein the step of populating the database of biometric signatures further comprises the step of enrolling a biometric signature into the database of biometric signatures comprising the steps of:

receiving a biometric signal; and

enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty.

[13] A non-transitory computer readable storage medium for storing a computer program comprising instructions, which when executed by processors causes the processors to perform the steps of the method of claim 10.

CHALLENGED CLAIMS OF THE '705 PATENT

[1pre] 1. A system for providing secure access to a controlled item, the system comprising:

[1a] a memory comprising a database of biometric signatures;

[1b] a transmitter sub-system comprising:

[1b1] a biometric sensor configured to receive a biometric signal;

[1b2] a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

[1b3] a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute; and

[1c] a receiver sub-system comprising: a receiver sub-system controller configured to:

[1c1] receive the transmitted secure access signal; and

[1c2] provide conditional access to the controlled item dependent upon said information;

[1d] wherein the transmitter sub-system controller is further configured to:

[1d1] receive a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

[1d2] map said series into an instruction; and

[1d3] populate the data base according to the instruction,

[1e] wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

[4] 4. The system according to claim 1, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern,

and palm configuration, and/or the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

[6a] 6. The system as claimed in claim 1, wherein the biometric sensor is further configured to authenticate the identity of a user;

[6b] wherein the transmitter is further configured to transmit information capable of granting access to the controlled item using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and

[6c] the system further comprising a control panel configured to receive the information and provide the secure access requested.

[10pre] 10. A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:

[10a] a biometric sensor configured to receiving a biometric signal;

[10b] a controller configured to match the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and

[10c] a transmitter configured to emit a secure access signal conveying said information dependent upon said accessibility attribute;

[10d] wherein the controller is further configured to:

[10d1] receive a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

[10d2] map said series into an instruction; and

[10d3] populate the database according to the instruction,

[10e] wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

[11pre1] 11. A method for providing secure access to a controlled item in a system comprising

[11pre2] a database of biometric signatures,

[11pre3] a transmitter sub-system comprising a biometric sensor configured to receive a biometric signal, and a transmitter configured to emit a secure access signal capable of granting access to the controlled item,

[11pre4] and a receiver sub-system comprising a receiver sub-system controller configured to receive the transmitted secure access signal, and provide conditional access to the controlled item dependent upon information in said secure access signal,

[11a] the method comprising: populating the database of biometric signatures by:

[11a1] receiving a series of entries of the biometric signal;

[11a2] determining at least one of the number of said entries and a duration of each said entry;

[11a3] mapping said series into an instruction; and

[11a4] populating the database according to the instruction;

[11b] receiving the biometric signal;

[11c] matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;

[11d] emitting a secure access signal conveying information dependent upon said accessibility attribute; and

[11e] providing conditional access to the controlled item dependent upon said information,

[11f] wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

[12] 12. The method according to claim 11, wherein populating the database of biometric signatures further comprises enrolling a biometric signature into the database of biometric signatures, and wherein enrolling the biometric signature into the database comprises:

receiving a biometric signal; and

enrolling the biometric signal as an administrator signature in response to the database of biometric signatures being empty.

[14pre] 14. A non-transitory computer readable storage medium storing a computer program comprising instructions, which when executed by processors causes the processors to:

[14a] receive a series of entries of a biometric signal;

[14b] determine at least one of a number of said entries and a duration of each of said entries;

[14c] map said series into an instruction;

[14e] populate a database of biometric signatures according to the instruction;

[14f] receive the biometric signal;

[14g] match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;

[14h] emit a secure access signal conveying information dependent upon said accessibility attribute; and

[14i] provide conditional access to a controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

[15pre] 15. A system for providing secure access to a controlled item, the system comprising:

[15a] a memory comprising a database of biometric signatures;

[15b] a transmitter sub-system comprising:

[15b1] a biometric sensor capable of receiving a biometric signal;

[15b2] a transmitter sub-system controller capable of matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

[15b3] a transmitter capable of emitting a secure access signal conveying information dependent upon said accessibility attribute; and

[15c] a receiver sub-system comprising: a receiver sub-system controller capable of:

[15c1] receiving the transmitted secure access signal; and

[15c2] providing conditional access to the controlled item dependent upon said information;

[15d] wherein the transmitter sub-system controller is further capable of:

[15d1] receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

[15d2] mapping said series into an instruction; and

[15d3] populating the data base according to the instruction,

[15e] wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

[16pre] 16. A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:

[16a] a biometric sensor capable of receiving a biometric signal;

[16b] a controller capable of matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and

[16c] a transmitter capable of emitting a secure access signal conveying said information dependent upon said accessibility attribute;

[16d] wherein the controller is further capable of:

[16d1] receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

[16d2] mapping said series into an instruction; and

[16d3] populating the database according to the instruction,

[16e] wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

[17pre1] 17. A method for providing secure access to a controlled item in a system comprising

[17pre2] a database of biometric signatures,

[17pre3] a transmitter sub-system comprising a biometric sensor capable of receiving a biometric signal, and a transmitter capable of emitting a secure access signal capable of granting access to the controlled item, and

[17pre4] a receiver sub-system comprising a receiver sub-system controller capable of receiving the transmitted secure access signal, and providing conditional access to the controlled item dependent upon information in said secure access signal,

[17a] the method comprising: populating the database of biometric signatures by:

[17a1] receiving a series of entries of the biometric signal;

[17a2] determining at least one of the number of said entries and a duration of each said entry;

[17a3] mapping said series into an instruction; and

[17a4] populating the database according to the instruction;

[17b] receiving the biometric signal;

[17c] matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;

[17d] emitting a secure access signal conveying information dependent upon said accessibility attribute; and

[17e] providing conditional access to the controlled item dependent upon said information,

[17f] wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

CERTIFICATE OF INTEREST

Case Number 24-1278, 24-1354

Short Case Caption CPC Patent Technologies Pty Ltd. v. Apple Inc.

Filing Party/Entity CPC Patent Technologies Pty Ltd.

Instructions:

1. Complete each section of the form and select none or N/A if appropriate.
2. Please enter only one item per box; attach additional pages as needed, and check the box to indicate such pages are attached.
3. In answering Sections 2 and 3, be specific as to which represented entities the answers apply; lack of specificity may result in non-compliance.
4. Please do not duplicate entries within Section 5.
5. Counsel must file an amended Certificate of Interest within seven days after any information on this form changes. Fed. Cir. R. 47.4(c).

I certify the following information and any attached sheets are accurate and complete to the best of my knowledge.

Date: 04/22/2024

Signature: /s/ George Summerfield

Name: George Summerfield

1. Represented Entities. Fed. Cir. R. 47.4(a)(1).	**2. Real Party in Interest.** Fed. Cir. R. 47.4(a)(2).	**3. Parent Corporations and Stockholders.** Fed. Cir. R. 47.4(a)(3).
Provide the full names of all entities represented by undersigned counsel in this case.	Provide the full names of all real parties in interest for the entities. Do not list the real parties if they are the same as the entities. ☑ None/Not Applicable	Provide the full names of all parent corporations for the entities and all publicly held companies that own 10% or more stock in the entities. ☑ None/Not Applicable
CPC Patent Technologies Pty Ltd.		

☐ Additional pages attached

4. Legal Representatives. List all law firms, partners, and associates that (a) appeared for the entities in the originating court or agency or (b) are expected to appear in this court for the entities. Do not include those who have already entered an appearance in this court. Fed. Cir. R. 47.4(a)(4).

☐ None/Not Applicable ☐ Additional pages attached

Brian P. Bozzo (K&L Gates LLP)		

5. Related Cases. Other than the originating case(s) for this case, are there related or prior cases that meet the criteria under Fed. Cir. R. 47.5(a)?

☑ Yes (file separate notice; see below) ☐ No ☐ N/A (amicus/movant)

If yes, concurrently file a separate Notice of Related Case Information that complies with Fed. Cir. R. 47.5(b). **Please do not duplicate information.** This separate Notice must only be filed with the first Certificate of Interest or, subsequently, if information changes during the pendency of the appeal. Fed. Cir. R. 47.5(b).

6. Organizational Victims and Bankruptcy Cases. Provide any information required under Fed. R. App. P. 26.1(b) (organizational victims in criminal cases) and 26.1(c) (bankruptcy case debtors and trustees). Fed. Cir. R. 47.4(a)(6).

☑ None/Not Applicable ☐ Additional pages attached

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Statutes

STATEMENT OF RELATED CASES

Pursuant to Federal Circuit Rule 47.5, counsel for Appellant states that: (a) no other appeal in or from the same proceeding was previously before this or any other appellate court, whether under the same or a similar title; and (b) the following cases will be directly impacted by this court's decision in the pending appeal:

Apple Inc. v. CPC Patent Technologies Pty Ltd., IPR2022-00601 (PTAB)

Apple Inc. v. CPC Patent Technologies Pty Ltd., IPR2022-00602 (PTAB)

Assa Abloy AB, et al. v. CPC Patent Technologies PTY, LTD., IPR2022-01094 (PTAB);

Assa Abloy AB, et al. v. CPC Patent Technologies PTY, LTD., IPR2022-01093 (PTAB);

Assa Abloy AB, et al. v. CPC Patent Technologies PTY, LTD., IPR2022-01006 (PTAB);

Assa Abloy AB, et al. v. CPC Patent Technologies PTY, LTD., No. 3:22-cv-00694 (D. Conn.);

CPC Patent Technologies PTY, LTD. v. Apple, Inc., 5:2022-cv-02553 (N.D. Cal.);

CPC Patent Technologies PTY, LTD. v. HMD Global Oy, 6:21-cv-00166 (W.D. Tex.);

CPC Patent Technologies PTY, LTD. et al v. HID Global Corp., 6-22-cv-01170 (W.D. Tex.)

JURISDICTIONAL STATEMENT

On September 27, 2023, the Board issued final written decisions ("FWDs") determining claims 1, 3–7, 9–11, and 13 of the '208 Patent and claims 1, 4, 6, 10–12, and 14–17 of the '705 Patent invalid. Appx1-65; Appx66-125. Regarding the '208 Patent, CPC timely requested director review on October 27, 2023, which was denied on November 6, 2023. Appx572-589; Appx590-592. On December 20, 2023, the same Board as in IPR2022-00601 determined the '208 Patent was not unpatentable as obvious in proceedings IPR2022-01045 and IPR2022-01089. Appx4399. CPC timely appealed from both decisions on December 18, 2023. Appx594.

Regarding the '705 Patent, CPC timely requested director review on October 4, 2023, which was denied on November 6, 2023. Appx3525-3541; Appx3542-3544. On November 30, 2023, the same Board as in IPR2022-00602 determined the '705 Patent was not unpatentable as obvious in IPR2022-01006. Appx4305. CPC sought a rehearing of the Director's decision to deny review in light of the same panel finding the same claims were not unpatentable in IPR2022-01006. Appx3546. This rehearing request was dismissed, noting "[a] party many not file a request for rehearing of the Director's decision to deny Director Review." Appx3555. CPC timely appealed on January 8, 2024. Appx3558.

This Court therefore has jurisdiction over this appeal pursuant to 28 U.S.C. § 1295(a)(4)(A) and 35 U.S.C. §§ 141(c) and 319.

INTRODUCTION

In its final written decisions invalidating every challenged claim, the Board routinely confused the input of biometric information, such as fingerprints, with the input of indisputably non-biometric information, such as a geometric pattern. This confusion infects the Board's analysis as to every challenged claim and warrants reversal.

In the IPR proceedings, Apple did not argue that swapping biometric signals for non-biometric ones would have been an obvious modification to the cited prior art. Apple also failed to present any evidence that replacing a post-enrollment process with an enrollment process would have been an obvious modification. Despite not making these arguments and not presenting this evidence, the Board improperly filled in the gaps for Apple. Troublingly, the Board's reasoning flies in the face of numerous instances of the parties' experts agreeing to the contrary.

Thus, the PTAB abused its discretion in finding that non-biometric signals equate to biometric signals, and that signal entries that occur after enrollment are nonetheless part of an enrollment process. Despite unrebutted evidence that the prior art fails to render the challenged claims obvious, the Board erroneously found each of the challenged claims unpatentable. Reversal is, therefore, warranted.

STATEMENT OF THE ISSUE

1. Whether the PTAB abused its discretion in finding that the proposed modification to Mathiassen's finger movements with Anderson's variable pressure pulses, both of which are non-biometric, and which are entered after an enrollment has taken place, nonetheless results in the claimed series of received biometric signal entries entered as part of an enrollment process, as required by the challenged claims.

STATEMENT OF THE CASE

A. The Challenged Patents

The '208 Patent, entitled "Remote Entry System," issued on February 23, 2016, from an application claiming priority of August 13, 2003. Appx126.

The '705 Patent is a continuation of the '208 Patent. Appx147. Like the '208 Patent, the '705 Patent claims priority of no later than August 13, 2003, and issued on May 30, 2017. Appx126.

The '208 and '705 Patents disclose a system 'for providing secure access to a controlled item.'" Appx5; Appx69. Claims 1 of the '208 and '705 Patents both further specify that the "controlled item" includes "an electronic lock on an electronic computing device." Appx145, 16:1-3; Appx166, 16:21-23. Claim 1 of the '208 Patent reads in its entirety as follows:

> 1. A system for providing secure access to a controlled item, the system comprising:
>
> a database of biometric signatures;

a transmitter sub-system comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;

and means for emitting a secure access signal conveying information dependent upon said accessibility attribute;

and a receiver sub-system comprising: means for receiving the transmitted secure access signal;

and means for providing conditional access to the controlled item dependent upon said information, wherein the transmitter sub-system further comprises means for populating the database of biometric signatures, the population means comprising:

means for receiving ***a series of entries of the biometric signal***,

said series being characterized according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction;

and means for populating the data base according to the instruction,

wherein the controlled item is one of a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

Appx145, 15:42-16:3 (emphasis added).

Claim 1 of the ’705 Patent reads in its entirety as follows:

1. A system for providing secure access to a controlled item, the system comprising:

a memory comprising a database of biometric signatures;

a transmitter sub-system comprising:

a biometric sensor configured to receive a biometric signal;

a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute; and

a receiver sub-system comprising: a receiver sub-system controller configured to: receive the transmitted secure access signal; and

provide conditional access to the controlled item dependent upon said information; wherein the transmitter sub-system controller is further configured to:

receive ***a series of entries of the biometric signal***,

said series being characterized according to at least one of the number of said entries and a duration of each said entry;

map said series into an instruction; and

populate the data base according to the instruction,

wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

Appx166, 15:62-16:23 (emphasis added).

The ’208 and ’705 Patents are designed to solve for the security problems associated with inputting secret digits or the use of a prior art biometric system. Appx138, 1:48-51. Of note for this appeal, the invention solves this problem, in part, by populating a database of biometric signatures that includes “receiving a series of entries of [a] ***biometric*** signal.” Appx139, 3:26-37 (emphasis added). As the PTAB recognized, the database is populated in this manner as part of a user enrollment process. Appx38; Appx97.

The challenged patents give an example of a “biometric” signal: the signal generated when a user presses his thumb on a “biometric sensor panel,” thereby allowing the authentication of the user’s “personal biometric identity.” Appx141, 7:43-51; *see also* Appx138, 1:29-30 (“One example of a biometric signal is a fingerprint”). In that regard, the PTAB also referenced a “succession of finger presses” applied to a “fingerprint sensor” as an example of the claimed “biometric signal.” Appx37.

As depicted graphically in the challenged patents, a biometric signal is first received at step 701 in Figure 6, and, if the database of biometric signals is empty at step 702, the invention proceeds to step 708 Figure 8 to commence the enrollment process. Appx133, Appx135. The latter figure shows the storage of the biometric signatures corresponding to the entered biometric signals at steps 804-807.

Appx135. For that enrollment process, the challenged patents explain that steps 805 and 807 in Figure 8 "involve ***sequences*** of finger presses on the biometric sensor." Appx143, 12:55-57 (emphasis added).

Fig. 8

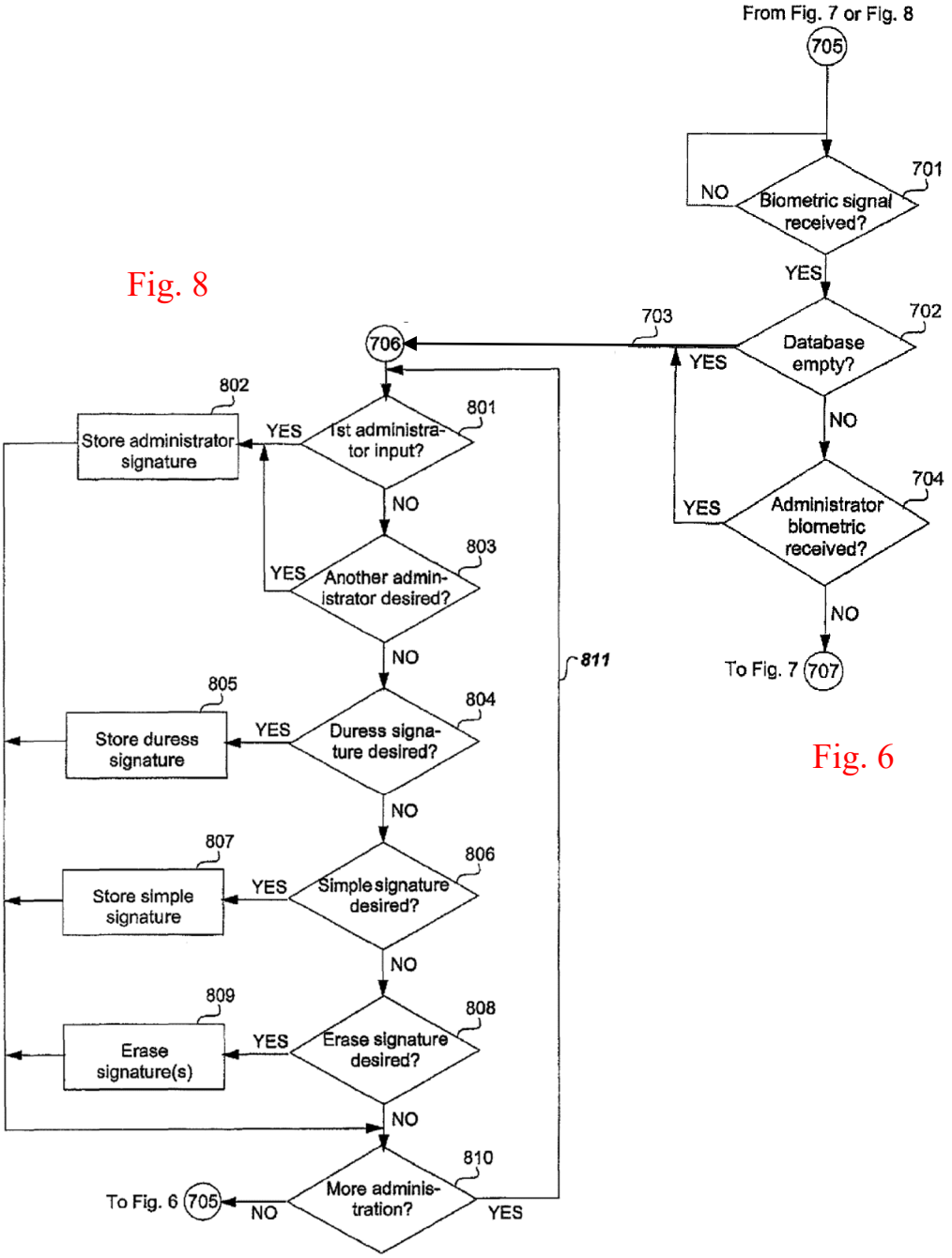


Fig. 6

Appx133, Appx135, Appx142, 10:5-19, Appx144, 13:7-19.

According to the plain language of claim 1 in both the '208 and '705 Patents, the series of biometric signal entries is characterized according to both "at least one of the number of said entries," as well as "***a duration*** of each said entry." Appx145, 15:62-64 (emphasis added); Appx166, 16:15-18 (same). In a co-pending district court matter between the parties, "[t]he court found the claim term 'at least' modifies 'one of the number of said entries' and that the claim requires 'a duration of each said entry.'" *See* Appx208 (citing Appx2247); Appx3240 (same).

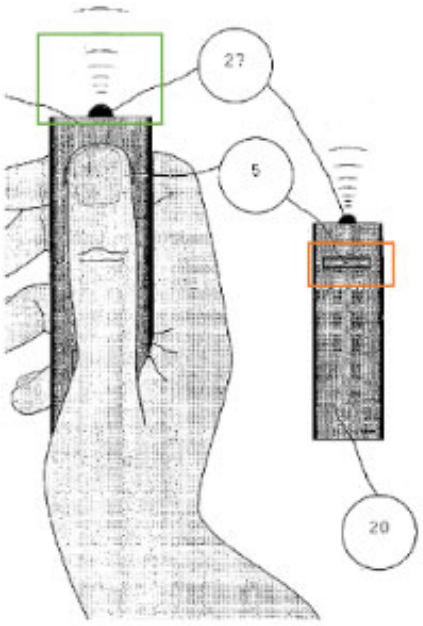
The PTAB observed that these "number and duration clauses" "require a number and duration of ***biometric*** signals because the input for these biometric signals is a biometric sensor, as disclosed in the Specification." Appx37 (emphasis added); Appx96 (same). As the PTAB recognized, "[i]f the number and duration of presses did not include a biometric component, it would be simply a 'knowledge-based' security measure, based on a pattern rather than based on a unique physical attribute of the user." Appx40; Appx99.

B. The Prior Art

Apple urged a single challenge ground: obviousness under 35 U.S.C. § 103(a) in light of Mathiassen, McKeeth, and Anderson. Appx40; Appx99. As will be demonstrated herein, that combination fails to teach a biometric signal series received as part of an enrollment process, as required by the subject claims.

1. Mathiassen

Mathiassen is generally "related to access and input devices for giving access and allowing user input in access limited devices, apparatuses, appliances, systems or networks." Appx1285, ¶ [0001]. While Mathiassen teaches several different embodiments of its access system, Apple relied upon the portable door control iteration, as depicted in Figure 8 of that reference, when mapping that reference to the challenged claims:



See, e.g., Appx190-191, Appx193; Appx3219, Appx3222.

This portable door control is part of the "automotive application" of Mathiassen's purported invention. Appx1295, ¶¶ [0146]-[0147]. Mathiassen teaches that a dealer will initially access a database on a separate computer terminal by "fingerprint authentication." *Id.*, ¶ [0152]. Mathiassen provides no description

of that authentication, *e.g.*, whether such authentication involves a "series" of fingerprint entries, and how the dealer's fingerprints are originally stored to allow for such authentication.

After such authentication, the following is Mathiassen's description of a user's fingerprint enrollment procedure:

> This first person to enroll his fingerprint on the portable door control (20) becomes the 'owner' of the car, in the sense that he becomes the system administrator. When he has successfully enrolled on the portable door control (20) he will countersign by his fingerprint to authorize and initiate encryption of his master minutiae table(s) from the IC (1) on the portable door control (20) via the door locks and the central car computer (not shown) to the IC (1) of the embedded ignition control (15) of the car.

Appx1296, ¶ [0165].

The master *minutiae* tables corresponding to the owner's fingerprints are then encrypted and transmitted to the central computer of the car. *Id.*, ¶ [0167]. As Apple admitted in its petition, "[a]lthough Mathiassen teaches inputting a command via a series of fingerprint representations, Mathiassen ***does not teach determining a duration of each entry***," meaning that these master *minutiae* tables do not include "duration" information. Appx180 (emphasis added); Appx3212 (same).

Separately, Mathiassen teaches, as an additional safety feature, the use of "omni-directional finger movements," which are compared to "***predefined*** sets of finger movement sequences including directional and touch/no-touch finger

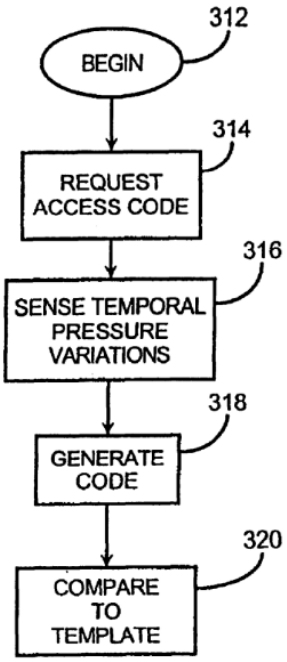
movement sequences," allowing for "controlling the device." Appx1297, ¶ [0192] (emphasis added). This capability additionally requires "[m]ovement analyzing means, in the form of a hardware or a software movement analyzing program module." *See id.*

While Mathiassen offers no express teaching regarding how or when these finger movement sequences are "predefined," this Court has affirmed that the plain and ordinary meaning of that term is to be "defined in advance." *See IGT v. Bally Gaming Int'l, Inc.*, 659 F.3d 1109, 1119 (Fed. Cir. 2011). In other words, nothing in Mathiassen expressly teaches that these predefined finger movements are stored in memory as part of the user's enrollment process.

2. Anderson

Anderson's invention relates to "systems employing user entered access codes such as passwords, personal identification numbers (PIN) and the like, and more particularly to a method for inputting such access codes via temporal variations in the amount of pressure applied to a touch interface." Appx1321, 1:7-12. As Anderson explains, its claimed method "includes the steps of sensing temporal variations in pressure applied to the touch interface, encoding the sensed temporal variations in pressure to generate a code, and comparing the generated code with a stored code template to determine if the code and the code template match within a predetermined tolerance." *Id.*, 2:7-12. Figure 3A shows the steps comprising that

method, including: 1) a user's attempt to access a function requiring an access code (step 312); 2) a request provided to the user to enter the access code (step 314); 3) the user's entered temporal pattern of pressure applications that is sensed by the touch interface (step 316); 4) an access code is generated (step 318); and 5) the generated access code is compared with a code template created earlier by the user (step 320).



See Appx1323, 5:58-6:27.

There is no biometric information involved in this process at all. In fact, Anderson teaches that fingerprint collection is an optional add-on to the procedure depicted in Figure 3A:

> [D]igitizer pad 120 ***may include*** an optical scanner or thermal sensor for collecting an image of the user's fingerprint as the pressure access code is entered and

> verified against a stored fingerprint template. Verification of both the collected fingerprint image and the access code ***may then be required*** before the user is allowed access to the system or information.

See Appx1324, 7:5-11 (emphasis added).

It is clear from the foregoing passage that the pressure pulses taught by Anderson are distinct from this optional fingerprint imaging, which is unsurprising, given that Anderson also teaches that fingerprint recognition utilizes "specialized equipment and may require sophisticated software for implementation." *See* Appx1321, 1:54-57. This discussion of fingerprint recognition appears in Anderson's Background of the Invention section, where Anderson is identifying the "drawbacks" of prior art security methods. And, as both parties' experts[1] opined, Anderson's pressure pulses are knowledge-based, rather than biometric:

Dr. Easttom

As Dr. Sears acknowledged and as discussed above, *Anderson's* pressure code is knowledge-based, not biometric. Ex. 2010 at 54:9-55:6. Dr. Sears is certainly correct that, if a sensor only captures the knowledge of a user, it is not properly characterized as a ***biometric*** sensor. *Id.* at 29:6-10. More specifically, a capacitive touch sensor that merely captures user taps or finger movements is not a biometric sensor. *Id.* at 36:1-9, 38:14-39:19.

Dr. Sears

Q. Would you characterize the pressure and duration patterns that Anderson teaches as knowledge-based?

A. Yes, I think when you start using things like the amount of pressure that you need to apply, and you might have a light pressure or more forceful pressure or a short contact or a long contact, that is starting to leverage some knowledge-based.

Appx2993, ¶ 69; Appx2894, 58:3-10.

---

[1] CPC presented testimony from Dr. Easttom, and Apple presented testimony from Dr. Sears.

In Anderson's teaching of optional fingerprint imaging, there is no disclosure in that reference as to the creation of the stored "template," let alone the specific entry of a ***series*** of fingerprint signals as part of an enrollment process to create that template. In fact, Anderson teaches "collecting ***an*** image of the user's fingerprint as the pressure access code is entered," as opposed to multiple images, belying any conclusion that Anderson captures a ***series*** of fingerprint signals as part of an enrollment process or otherwise. *See* Appx1324, 7:6-7 (emphasis added).

3. McKeeth

McKeeth's teachings are directed to "authenticating a user to access a computer system" using an "implicit input" to match with "corresponding information associated with the user," and "granting the user access to the computer system in the event of a satisfactory match." Appx1302, Abstract. McKeeth gives as an example of "implicit input" forming a geometric pattern using a mouse. Appx1308, 4:5-9. McKeeth contrasts its invention with fingerprint authentication, which is "not immune to the computer hacker's ability to force the user to place his/her finger on the acquisition device," or to "provide a simulated [fingerprint] signal to the computer system to obtain access." Appx1307, 1:49-55.

McKeeth goes on to teach that combinations of "input signals may be used to authenticate a user," including "a password from a keyboard," "a fingerprint scan from an optical scanner," and "a geometric pattern from a mouse or trackball."

Appx1308, 3:11-18. The user can, for example, "enter a password through the keyboard and, within a predetermined duration of time (e.g., 5 seconds), ***place his/her finger on the mouse to be scanned while moving the mouse in a specified pattern***." *Id.*, 3:19-23 (emphasis added).

McKeeth makes clear that the invention described operates when the user performs "a fingerprint scan and/***or*** pattern," indicating that the fingerprint scan and geometric pattern are separate operations. *See id.*, 3:40-53 (emphasis added). As Figures 3A-3D illustrate, the geometric patterns are ***not*** biometric, as they are patterns that can be learned:

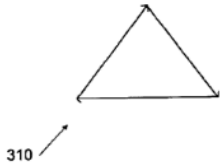


FIG. 3A

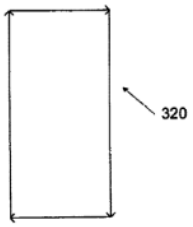


FIG. 3B

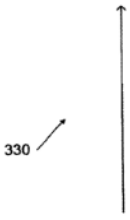


FIG. 3C

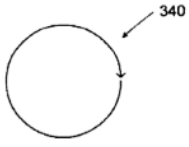


FIG. 3D

Appx1305, Figs 3A-3D. In fact, McKeeth teaches that these geometric figures are formed by moving a trackball over a flat surface, so ***no*** fingerprint data is collected in forming these figures. *See* Appx1309, 5:34-40.

C. Procedural Background

As noted above, Apple petitioned for review of the challenged patents on a single obviousness challenge ground involving the three afore-discussed references. *See, e.g.*, Appx40; Appx99. CPC urged in response that the asserted combination failed to teach a "duration" component for the claimed ***biometric*** signal series, as any duration present would be, at most, attendant to a non-biometric signal, *i.e.*, Anderson's knowledge-based pressure pulses, or geometric designs of the type disclosed in Mathiassen and McKeeth. *See* Appx58; Appx116-117. Further, CPC maintained that there is no teaching that the combination referenced by Apple is part of an enrollment process, as required by the challenged claims. *See* Appx60; Appx121.

In finding all challenged claims unpatentable, the PTAB made two critical, and erroneous, findings: 1) "there can be no reasonable dispute that Anderson discloses input ***biometric*** signals that vary in number and duration" (Appx57 (emphasis added); Appx116); and 2) "[b]ecause Mathiassen, like the [challenged patents], uses a biometric sensor as the input device, it will detect the biometric part of the input signal, while also sensing the number and duration of inputs" (Appx58; Appx117).

As to the first finding, the PTAB cited to Anderson's teaching "of inputting an access code" using a digitizer pad "as a touch interface, which ***may*** include an

optical scanner or thermal sensor for collecting an image of the user's fingerprint." Appx44 (emphasis added); Appx103. The PTAB did not address the fact that inputting an access code on Anderson's digitizer pad could occur with or without simultaneous fingerprint imaging, *i.e.*, the former is not a biometric signal even if the latter is.

As to the second point, the PTAB failed to address Mathiassen's express teaching that movement detection (including "touch/no-touch finger movement sequences") additionally requires "[m]ovement analyzing means, in the form of a hardware or a software movement analyzing program module," and particularly how that movement analyzing means corresponds to anything in the challenged patents. *See* Appx1297, ¶ [0192].

Finally, the PTAB provided no explanation as to how Mathiassen's finger movement sequences or Anderson's touch sequences are part of an enrollment process, despite the PTAB's express acknowledgement that "populating" the database with the received biometric information in the challenged claims is part of such a process. *See* Appx38; Appx97.

After the PTAB issued its Final Written Decisions, CPC sought Director review of, *inter alia*, whether the prior art taught the entry of the claimed biometric signal series as part of an enrollment procedure. Appx573; Appx3526. The Director denied both requests on November 6, 2023. Appx591; Appx3543. CPC timely filed

its notice of appeal in the IPR2022-00601 proceeding on December 18, 2023. Appx594.

In the IPR2022-00602 proceeding, CPC sought a rehearing of the Director's decision to deny review in light of the same panel finding the same claims were not unpatentable in IPR2022-01006. Appx3546. This rehearing request was dismissed, noting "[a] party many not file a request for rehearing of the Director's decision to deny Director Review." Appx3555. CPC timely filed its notice of appeal in the IPR2022-00602 proceeding on January 8, 2024. Appx3558. The Court consolidated the proceedings on January 25, 2024. ECF No. 10, 1.

SUMMARY OF ARGUMENT

Apple's proposed combination of Mathiassen/McKeeth/Anderson fails to teach "a series of entries of the biometric signal" as part of an enrollment process, as required by the challenged claims. In urging its sole challenge ground, Apple must resort to non-biometric signaling to satisfy the "biometric" signal series requirement of such claims, specifically the finger movement sequences of Mathiassen and the variable pressure sequences of Anderson. There is no dispute that these sequences are knowledge-based – they can be learned by anyone. In fact, both parties' experts ***agree*** on this point. However, because of the paucity of teachings in the cited prior art regarding fingerprint imaging, which would be biometric, Apple is required to rely upon these non-biometric features.

Further, and separately, there is no teaching in either Mathiassen or Anderson regarding these sequences being part of a user enrollment process, as required by the challenged claims. In both instances, the teachings of these references relate to functionality available ***after*** a user has been enrolled. Mathiassen teaches "predefined" finger movements stored for comparison purposes with no explanation as to how that predefinition occurred. Similarly, Anderson references a "stored" fingerprint template with no indication as to how such template was created. The absence of any tether between these teachings and a user enrollment process evinces reversible error in the PTAB's decision finding the challenged claims unpatentable.

ARGUMENT

I. STANDARD OF REVIEW

This Court reviews the PTAB's factual findings for substantial evidence and its legal determinations *de novo*. *See, e.g., In re Van Os*, 844 F.3d 1359, 1360 (Fed. Cir. 2017). Obviousness, the sole basis for rejecting the proposed claims below, is a question of law based on subsidiary findings of fact. *Id.* The PTAB "must make findings of relevant facts, and present its reasoning in sufficient detail that the court may conduct meaningful review of the agency action." *In re Lee*, 277 F.3d 1338, 1346 (Fed. Cir. 2002); *see also In re NuVasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) ("The PTAB must provide 'a reasoned basis for the agency's action….'").

II. THE PRIOR ART'S NON-BIOMETRIC, POST-ENROLLMENT DISCLOSURE DOES NOT RENDER OBVIOUS A METHOD OF ENROLLING BIOMETRIC DATA

As the PTAB noted, "[t]he question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when available, evidence such as commercial success, long felt but unsolved needs, and failure of others." Appx12 (citation omitted); Appx77. Here, the subject differences are the claimed "biometric" signal series in the challenged claims versus the non-biometric signals in the prior art, and the claimed use of such series as part of an enrollment process versus the prior art's use of a signals used *after* an enrollment process.

"Illustrative" claim 1 of each of the challenged patents requires receiving "a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry." Appx10; Appx75. This function is part of the "enrolling feature." Appx38; Appx97.

Apple admitted that "Mathiassen does not teach determining a duration of each entry." Appx180; Appx3212. Therefore, Apple relied upon Anderson as purportedly teaching "receiving a series of fingerprint pressure pulses of varying duration." Appx231; Appx3242-3243. The substitution proposed by Apple, and found invalidating by the PTAB, involves modifying Mathiassen's directional finger

movements with a series of presses of varying duration, as taught by Anderson. *See* Appx57; Appx116. There are two clear errors underlying this finding: 1) the combination in question is entirely non-biometric, as both Mathiassen's finger movements and Anderson's finger presses are knowledge-based; and 2) neither Mathiassen's finger movements nor Anderson's finger presses are part of an enrollment process. Either error is sufficient to reverse the PTAB's ruling that the challenged claims are unpatentable.

A. Apple's Cited Prior Art Combination Results in a Non-Biometric Signal Series

As discussed above, the PTAB's invalidity finding hinges upon a combination of Mathiassen's finger movements and Anderson's series of pressure pulses, the latter purportedly providing the required "duration" component to the claimed signal series. Both of these features are indisputably non-biometric.

Beginning with Mathiassen's finger movements, CPC's expert provided the non-controversial opinion that such movements, which can be learned, are not biometric:

> To one of ordinary skill in the art, the finger movements suggested in Mathiassen, as distinct from fingerprints themselves, are not biometric signals, as something more than the fingerprint sensor is required to track them, and one can "learn" finger movements. Fingerprints are unique to a specific individual; finger movements are not. Anyone can duplicate [a] particular set of finger movements. One of ordinary skill in the art would understand that, in the context of tracking 'omni-

> directional finger movements,' the fingerprint sensor, in conjunction with the translation means hardware or software, is not acting like a fingerprint sensor.

Appx2987-2988, ¶ 53.

Apple's own expert also acknowledged that Mathiassen's movement analyzing means was concerned with finger movement, as opposed to the fingerprints themselves. *See* Appx3097-3098, 51:4-52:6. Even the PTAB appeared to agree, stating "there can be no reasonable dispute that Mathiassen discloses a computer implemented software translation program for converting finger ***movements*** into control signals." Appx59 (emphasis added); Appx120.

While Apple does not rely on the McKeeth reference for the "duration" limitation, that reference also shows how geometric patterns are non-biometric, requiring no fingerprint information at all. *See* Appx1309, 5:34-40 (using a trackball to form geometric patterns). And, as CPC's expert noted, McKeeth's geometric patterns are "knowledge-based," irrespective of the mechanism used to form them. Appx2985-2986, ¶ 47. McKeeth's teaching is therefore analogous to Mathiassen's knowledge-based finger movements.

Yet, the PTAB noted that "[a] fingerprint sensor's ability to recognize a fingerprint is not turned off when a succession of finger presses is applied to the fingerprint sensor." Appx37; Appx96. Contrary to the PTAB's finding, however, the issue is not whether Mathiassen's sensor is "turned off" when a user employs

finger movements. Indeed, in three separate *inter partes* reviews finding the same claims of the ***same*** patents *patentable*, the same panel found that the prior art cited therein uses "the same biometric (fingerprint) sensor for the ***dual purposes*** of (i) reading fingerprints for authentication and access control and (ii) as a means of issuing commands/instructions through a series of 'taps' of varying durations." Appx4385-4386 (emphasis added); Appx4295 (same, internal citation omitted).[2]

The issue, rather, is whether the fingerprint sensor is operating for the first purpose – "reading fingerprints for authentication and access control" – when it analyzes finger movements (*e.g.*, taps) pursuant to the sensor's second purpose. Both experts agree that it does not, and Mathiassen's finger movements are non-biometric, as anyone can learn them. Appx2987-2988, ¶ 53; Appx3097-3098, 51:4-52:6.

[2] These decisions were vacated by the Director on other grounds, namely the panel's construction of "biometric signal" which the Director determined was improperly issued for the first time in the final written decisions. *Assa Abloy AB, et al. v. CPC Patent Technologies PTY, LTD.*, IPR2022-01006, -01045, -01089, Paper 49 at 6-7 (P.T.A.B. Mar. 15, 2024) ("The Board's construction of 'biometric signal' in its Final Written Decisions, however, requires that the biometric signal 'provides secure access to a controlled item.' Neither party's proposed construction includes a requirement of 'provid[ing] secure access to a controlled item.' Nor was this requirement articulated in the Board's preliminary construction in its institution decision, where it afforded the term its 'plain and ordinary meaning.'" (internal citations omitted)).

Turning now to Anderson's variable duration finger presses, which Apple relies upon as the purported "duration" component of the biometric signal series, the analysis is essentially the same as with Mathiassen's finger movements. Both experts agree that the duration pattern of Anderson's finger presses are knowledge-based, *i.e.*, they are non-biometric. *See* Appx2993, ¶ 69 ("As Dr. Sears acknowledged and as discussed above, Anderson's pressure code is knowledge-based, not biometric."); Appx2894, 58:3-10 ("Q. Would you characterize the pressure and duration patterns that Anderson teaches as knowledge-based? A. Yes, I think when you start using things like the amount of pressure that you need to apply, and you might have a light pressure or more forceful pressure or a short contact or a long contact, that is starting to leverage some knowledge-based."). Nonetheless, the PTAB contended that "there can be no reasonable dispute that Anderson discloses input ***biometric*** signals that vary in number and duration."[3] Appx57 (emphasis added); Appx116. As support, the PTAB cited Apple's contention that "Anderson…teaches receiving a series of ***fingerprint*** pressure pulses of varying duration." *Id.* (emphasis added). The passage from Anderson cited in Apple's Petition is the following:

---

[3] The Panel elsewhere appears to recognize that this statement is erroneous, as it states that Anderson only contributes "a number and duration of pulses as inputs," while the combination of Mathiassen and McKeeth actually provides a teaching of "biometric sensing." Appx58; Appx117.

> As shown in FIG. 4A, the touch interface may sense only temporal applications of pressure relying on timing of the pressure applications for entry of the access code. In such an embodiment, the touch interface would not detect variations in pressure magnitude or intensity. Thus, the access code would be entered as a series of alternating pressure applications of varying duration.

Appx210 (citing Appx1324, 7:28-34); *see also* Appx3243-3244.

There is no mention of fingerprints in this passage.[4] Indeed, Anderson's teachings of fingerprint imaging, apart from denigrating that technology, is "collecting ***an*** image of the user's fingerprint as the pressure access code is entered." Appx1324, 7:4-7 (emphasis added). There is no mention in Anderson of a series of fingerprint entries, let alone a duration associated with each such entry.

Further, as the PTAB noted in the co-pending *inter partes* reviews, a single sensor can both read fingerprints and simultaneously issue commands through "a series of 'taps' of varying duration," which is precisely Anderson's teaching. *See* Appx4385-4386; Appx4295.[5] This holding confirms the two concepts – fingerprint recognition and capturing a series or taps or other inputs – are distinct in the art. Yet, while the PTAB found the claims of the '208 and '705 Patents patentable in those

---

[4] The PTAB also mistakenly adopts Apple's references to a "fingerprint access code" (Appx44; Appx103) and a "series of fingerprint pressure pulses of varying duration" (Appx57; Appx115-116), purportedly found in Anderson's teachings. Neither of these terms appear anywhere in that reference, however.

[5] Vacated on other grounds. *Assa Abloy*, IPR2022-01006, -01045, -01089, Paper 49 at 7.

co-pending actions, it reached the opposite conclusion here, failing to recognize the similar dual purpose of Anderson's sensor.

The upshot of the foregoing is that Apple's proposed combination of Mathiassen's non-biometric finger movements with Anderson's non-biometric variable pressure taps necessarily results in a non-biometric signal series. As the challenged claims call for "a series of entries of the ***biometric*** signal," this proposed combination does not render obvious such claims, which was, in fact, the result in co-pending *inter partes* reviews. Appx4395-4396 (agreeing with Patent Owner that "[b]ecause the '208 Patent claims require entries of a biometric signal that is characterized by a number and a duration, the finger presses of Mathiassen[-067] – which are not biometric entries at all – do not teach or suggest these '208 Patent claim limitations."); Appx4302-4303 (same for the '705 Patent).[6] The PTAB abused its discretion in finding the challenged claims unpatentable.

B. Mathiassen's Finger Movements and Anderson's Variable Pressure Pulses Are Not Part of an Enrollment Process

The challenged claims further require populating a database of biometric signatures by "receiving a series of entries of [a] biometric signal" as part of a user enrollment process. Appx38; Appx97; *see also* Appx139, 3:26-37. Mathiassen

[6] Vacated on other grounds. *Assa Abloy*, IPR2022-01006, -01045, -01089, Paper 49 at 7.

teaches the use of "omni-directional finger movements," which are compared to "***predefined*** sets of finger movement sequences including directional and touch/no-touch finger movement sequences," allowing for "controlling the device." Appx1297, ¶ [0192] (emphasis added). A "command table" in Mathiassen "is used to translate the categorized finger movements into control signals whereby the translating means generates control signal" resulting in such control. *Id.*

There is no teaching in Mathiassen that these finger movements are part of an enrollment process as required by the challenged claims, or that the finger movements are used to populate a database. The PTAB nonetheless credited Apple's argument that "Mathiassen's fingerprint sensor receives this series of entries of the biometric signal, similar to the '208 Patent's code entry module 103 containing a biometric sensor 121 that receives a user's fingerprint." Appx61; Appx122. Putting aside the dual purpose served by Mathiassen's sensor when imaging a fingerprint while simultaneously collecting non-biometric signals, the PTAB simply ignores ***when and whether*** Mathiassen's sensor collects such signals, focusing only upon ***how*** it does so.

This omission is particularly surprising, given the PTAB's cognizance of CPC'S contention that "Mathiassen has no teaching that either the 'predefined sets of finger movement sequences' or the 'command table' constitute a series of received biometric signal entries that are mapped into an instruction used to populate

the database ***as part of the enrollment process***." Appx60 (emphasis added); Appx121. The PTAB's failure to address CPC's argument other than to summarize and tacitly reject it was an abuse of discretion. *See In re Nuvasive*, 842 F.3d at 1383 ("it is not adequate to summarize and reject arguments without explaining why the PTAB accepts the prevailing argument").

The PTAB also references Mathiassen's master *minutiae* tables, which are generated as part of a user enrollment process. *See, e.g.*, Appx60; Appx120-121. However, such tables are ***not*** the feature from Mathiassen that Apple proposes modifying with Anderson's pressure pulses. Appx215-216 ("*Mathiassen* teaches instructing a particular command with a series of fingerprint representations, and *Anderson* teaches enabling a requested function via a series of fingerprint pulses of varying durations."); Appx3249 (same). The PTAB ultimately recognizes this in referencing Mathiassen's finger movements as the "series of entries of the biometric signal" that is received by Mathiassen's sensor, rather than the generation of the master minutiae tables. *See* Appx60-61; Appx122. In short, nothing in Mathiassen ties the finger movements taught in that reference to an enrollment process.

Turning now to Anderson's series of variable pressure pulses, the following description thereof by the PTAB is telling:

> Anderson's method of inputting an access code uses digitizer pad 120 as a touch interface, which may include an optical scanner or thermal sensor for collecting an image of the user's fingerprint. [Appx1323], 5:43-44, 7:4-

> 7. The user enters the access code as a series of pressure pulses having varying durations. *Id.* at 6:45-47. This fingerprint access code is then compared with ***a stored code template*** to determine whether they match. If they do, access is permitted. *Id.* at 6:48-54.

Appx44 (emphasis added); Appx103.

Similarly, Anderson teaches "collecting an image of the user's fingerprint as the pressure access code is entered and verified against a ***stored fingerprint template***." Appx1324, 7:4-8 (emphasis added). With both the pressure pulses and the fingerprint image, the comparison is to a ***pre-stored*** template, making clear that the pressure pulses and fingerprint imaging referenced in Anderson are captured after user enrollment has occurred. As with Mathiassen, nothing expressly taught in Anderson relates to an enrollment process.

III. THE PTAB'S ERROR WARRANTS REVERSAL

The foregoing makes clear that the PTAB abused its discretion in finding that non-biometric signals equate to biometric signals, and that signal entries that occur after enrollment are nonetheless part of an enrollment process. Apple did not argue, and the PTAB did not find, that swapping biometric signals for non-biometric ones would have been an obvious modification to the cited prior art combination. Nor was there any evidence that replacing a post-enrollment process with an enrollment process would have been an obvious modification. Thus, in light of the sole challenge ground that Apple urged – a combination of non-biometric signals entered

post enrollment, there would be nothing remaining for the PTAB to do on remand. The necessary result, then, in light of the PTAB's abuse of discretion would be to reverse the PTAB's decision and find that the challenged claims are patentable.

CONCLUSION

For the foregoing reasons, the PTAB's decision that the challenged claims of the '208 and '705 Patents are obvious should be reversed.

Dated: April 22, 2024

Respectfully submitted,

By: /s/ George C. Summerfield

GEORGE C. SUMMERFIELD
george.summerfield@klgates.com
JONAH B. HEEMSTRA
jonah.heemstra@klgates.com
K&L GATES LLP
70 West Madison Street
Chicago, Illinois 60602-4207
(312) 372-1121

DARLENE F. GHAVIMI-ALAGHA
darlene.ghavimi@klgates.com
K&L GATES LLP
2801 Via Fortuna, Suite 650
Austin, Texas 78746
(512) 482-6800

ATTORNEYS FOR APPELLANT
CPC PATENT TECHNOLOGIES PTY, LTD.

ADDENDUM

INDEX TO ADDENDUM

Trials@uspto.gov
571-272-7822

Paper 31
Date: September 27, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

CPC PATENT TECHNOLOGIES PTY, LTD.,
Patent Owner.

IPR2022-00601
Patent 9,269,208 B2

Before SCOTT A. DANIELS, BARRY L. GROSSMAN, and AMBER L. HAGY, *Administrative Patent Judges.*

GROSSMAN, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

A. Background and Summary

Apple Inc. ("Petitioner" or "Apple") filed a Petition requesting *inter partes* review of claims 1, 3–7, 9–11, and 13 (collectively, the "challenged claims") of U.S. Patent No. 9,269,208 B2 (Ex. 1001, "the '208 patent"). Paper 1 ("Pet."). CPC Patent Technologies PTY, Ltd. ("Patent Owner" or "CPC") filed a Preliminary Response to the Petition. Paper 7 ("Prelim. Resp."). With our authorization, Petitioner filed a Preliminary Reply (Paper 8 ("Prelim. Reply")) addressing the issue of discretionary denial raised in the Preliminary Response and Patent Owner filed a Prelim. Sur-Reply (Paper 9 ("Prelim. Sur-Reply")).

We concluded that Petitioner satisfied the burden, under 35 U.S.C. § 314(a), to show that there was a reasonable likelihood that Petitioner would prevail with respect to at least one of the challenged claims. Accordingly, on behalf of the Director (37 C.F.R. § 42.4(a)), and in accordance with *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1353 (2018), we instituted an *inter partes* review of all the challenged claims, on the single asserted ground. Paper 11 ("Dec. Inst.").

Patent Owner filed a Response. Paper 17 ("PO Resp."). Petitioner filed a Reply. Paper 20 ("Reply"). Patent Owner filed a Sur-reply. Paper 26 ("Sur-reply").

Petitioner submitted seventy-six exhibits. *See* Exs. 1001–1091[1] (some consecutive exhibit numbers were *not* used; *e.g*, there are no exhibits

[1] Exhibit 1091 is a demonstrative exhibit used at the final hearing. It is not an evidentiary exhibit. *See* PTAB Consolidated Trial Practice Guide, 84 (Nov. 2019 ("TPG") ("Demonstrative exhibits used at the final hearing are aids to oral argument and not evidence.").

numbered 1056–1064); *see also* Paper 28 (Petitioner's Updated Exhibit List stating that Exhibit numbers 1056–1064 were "Intentionally left blank."). Petitioner relies on the Declaration testimony of Andrew Sears, Ph.D. *See* Exs. 1003, 1090.

Patent Owner submitted fourteen exhibits. *See* Exs. 2001–2014[2]; *see also* Paper 29 (Patent Owner's Updated Exhibit List). Petitioner relies on the Declaration testimony of William C. Easttom III, D. Sc., Ph.D. *See* Exs. 2011, 2012.

A hearing was held June 29, 2023. *See* Paper 30 ("Transcript" or "Tr.").

We have jurisdiction under 35 U.S.C. § 6. We enter this Final Written Decision pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

Petitioner has the burden of proving unpatentability of a claim by a preponderance of the evidence. 35 U.S.C. § 316(e).

Based on the findings and conclusions below, we determine that Petitioner has proven that claims 1, 3–7, 9–11, and 13 are unpatentable.

B. Real Parties-in-Interest

Apple identifies itself as the sole real party-in-interest. Pet. 72.

CPC also identifies itself as the sole real party-in-interest. Paper 4, 2.

There is no dispute between the parties concerning the real party-in-interest.

C. Related Matters

Petitioner and Patent Owner each identify the following two district court proceedings as related matters: (1) *CPC Patent Technologies Pty Ltd.*

[2] Exhibit 1014 is a demonstrative exhibit used at the final hearing. It is not an evidentiary exhibit. *See id.*

v. Apple Inc., Case No. 6:21-cv-00165-ADA (W.D. Tex.); and (2) *CPC Patent Technologies Pty Ltd. v. HMD Global Oy,* Case No. 6:21-cv-00166-ADA (W.D. Tex.) (the "*HMD* Litigation"). Pet. 72; Paper 4, 2–3.

The first listed case, between the same parties involved in this *inter partes* review proceeding, however, has been transferred to the Northern District of California. *See In re Apple Inc.*, 2022 WL 1196768 (Fed. Cir. Apr. 22, 2022); *see also* Ex. 3002 (Text Order granting Motion to Change Venue). The case is now styled *CPC Patent Technologies Pty Ltd. v. Apple Inc.*, No. 5:22-cv-02553 (N.D. Cal.). *See* Ex. 3003 (PACER Docket for the transferred case); Prelim. Resp. 1, fn 1 (Patent Owner acknowledging the transfer from the Western District of Texas to the Northern District of California). Also, the '208 patent is no longer involved in the Northern District of California case. Patent Owner states it "dismissed its infringement claim for the '208 Patent in the district court action." Prelim. Resp. 1.

Petitioner and Patent Owner also each identify the following two pending *inter partes* review proceedings as related matters: (1) IPR2022-00600, challenging claims in Patent 8,620,039; and (2) IPR2022-00602, challenging claims in Patent 9,665,705, which is based on a continuation of the application that matured into the '208 patent in the proceeding before us. *See* Ex. 3001, code (63). A final written decision in the 00600 IPR is due October 17, 2023. A final written decision in the 00602 IPR is being issued simultaneously with this Decision in the case before us.

D. The '208 Patent

We make the following findings concerning the disclosure of the '208 patent.

The '208 patent discloses a system "for providing secure access to a controlled item." Ex. 1001, Abstr. Examples of a "controlled item" include "a door locking mechanism on a secure door, or an electronic key circuit in a personal computer" that can be accessed only by an authorized user. Ex. 1001, 6:13–16. The system uses a database of "biometric signatures," such as a fingerprint, for determining authorized access. *Id.* at 1:29–30; 5:63–65 ("the user database [ ] contains biometric signatures for authorised[3] users against which the request [ ] can be authenticated").

Figure 2 from the '208 patent is reproduced below.

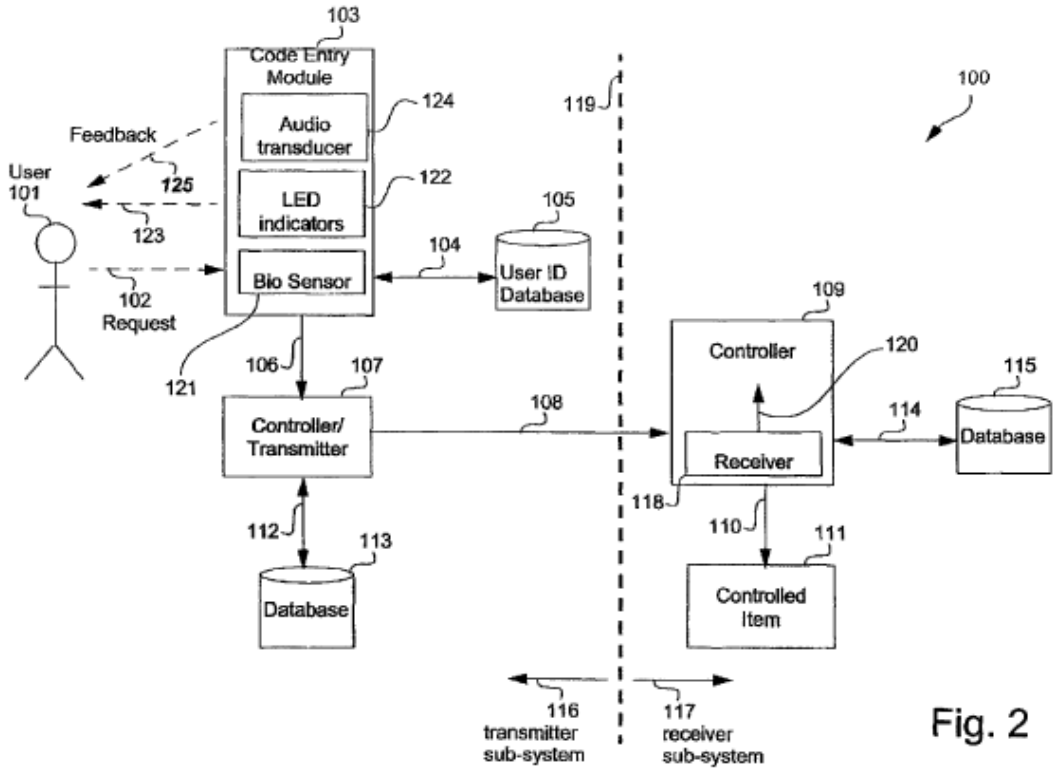


Fig. 2

[3] The Specification uses the British spelling, which we also use when quoting the Specification.

Figure 2 is a functional block diagram of an arrangement for providing secure access according to the system disclosed in the '208 patent. Ex. 1001, 5:15–16.

As described in the written description of the '208 patent, and as illustrated generally in Figure 2, user 101 makes request 102 to "code entry module 103." *Id.* at 5:51–55. Code entry module 103 includes biometric sensor 121. *Id.* The specific type of biometric sensor 121 used depends on the type of request 102, or biometric input signal, to be used. *Id.* If biometric sensor 121 is a fingerprint sensor, for example, then biometric input signal 102 "typically takes the form of a thumb press" on a sensor panel (not shown) on code entry module 103. Ex. 1001, 5:56–59. 403. "Other physical attributes that can be used to provide biometric signals include voice, retinal or iris pattern, face pattern, [and] palm configuration." *Id.* at 1:30–32.

Code entry module 103 then "interrogates" authorized user identity database 105, which contains "biometric signatures" for authorized users, to determine if user 101 is an authorized user. *Id.* at 5:60–65. Database 105 is prepared by an "administrator." *Id.* at 10:28–34 ("The first user of the code entry module 103 . . . is automatically categorised as an administrator.").

The disclosed system and method compare biometric input "*signal*" 102 to database 105 of authorized biometric "*signatures*" to determine if user 101 is an authorized user. *Id.* at 5:61–65 ("Thus for example if the request 102 is the thumb press on the biometric sensor panel 121 [producing a thumbprint] then the user database 105 contains biometric signatures [*i.e.,* thumbprints] for authorised users against which the request 102 can be authenticated."). If user 101 is an authorized user, code entry module 103

sends a signal to "controller/transmitter" 107 allowing access to the controlled item. *Id.* at 5:65–67.

When biometric sensor 121 is a fingerprint sensor,[4] the biometric signatures stored in database 105 are not limited to a single fingerprint. The '208 patent also discloses that, if so programed by an administrator, code entry module 103 may be activated by providing a succession of finger presses to biometric sensor 121 included in module 103. *Id.* at 10:45–47. If these successive presses are of the appropriate duration, the appropriate quantity, and are input within a predetermined time, controller 107 accepts the presses "as potential control information," or a biometric signal, and checks the input information against a stored set of "legal [authorized] control signals," or the database of biometric signatures. *Id.* at 10:47–67. "In one arrangement, the control information is encoded by *either or both* (a) the number of finger presses and (b) the relative duration of the finger presses." *Id.* at 10:49–52 (emphasis added).

An example of this type of "control information" or "legal control signal" is "dit, dit, dit, dah," where "dit" is a finger press of one second's duration and "dah" is a "finger press of two second's duration."[5] *Id.* at 10:57–63.

---

[4] *See* Ex. 1001, 10:35 – 38 ("Although the present description refers to 'Users', in fact it is 'fingers' which are the operative entities in system operation *when the biometric sensor 121 (see FIG. 2) is a fingerprint sensor*.") (emphasis added). Thus, it is clear that biometric sensor 121 is *not* limited to a fingerprint sensor.

[5] We have not been directed to any persuasive evidence, and have found none on our own review of the evidence, which establishes why the Specification refers to the number and duration of finger presses as "control information" and "legal control signals," rather than a "biometric signal" and a "database" of "biometric signatures," respectively, which are the terms

If user 101 is an authorized user based on the inputs to code entry module 103, controller/transmitter 107 then sends "an access signal," based on a "rolling code," to controller 109. Ex. 1001, 6:1–5. According to the written description, "[t]he rolling code protocol offers non-replay encrypted communication." *Id.* at 6:5–6. Other secure codes, such as "the Bluetooth™ protocol, or the Wi Fi™ protocols" also can be used. *Id.* at 6:28–34.

If controller 109 determines that the rolling code received is "legitimate," then controller 109 sends a command to "controlled item 111," which, for example "can be a door locking mechanism on a secure door, or an electronic key circuit in a personal computer" that is to be accessed by user 101. *Id.* at 6:7–16.

Code entry module 103 also incorporates at least one mechanism for providing feedback to user 101. *Id.* at 6:20–21. This mechanism can, for example, take the form of "one or more Light Emitting Diodes (LEDs) 122," and/or audio transducer 124, which provide visual or audio feedback to the user. Ex. 1001, 6:22–27.

---

used throughout the Specification for the input signal and the database of authorized users.

The Specification is required to include "a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art . . . to make and use the same." 35 U.S.C. § 112(a). Neither we nor the parties, however, have jurisdiction in this *inter partes* review proceeding to address an enablement issue. *See id.* at § 311(b) ("A petitioner in an inter partes review may request to cancel as unpatentable 1 or more claims of a patent only on a ground that could be raised under section 102 or 103 and only on the basis of prior art consisting of patents or printed publications.").

In Figure 2, "sub-system 116," shown on the left of vertical dashed line 119, communicates with "sub-system 117," shown on the right of dashed line 119, "via the wireless communication channel" used by access signal 108 between controller/transmitter 107 and controller/receiver 109. *Id.* at 6:62–65. As disclosed in the '208 patent, "[a]lthough typically the communication channel uses a wireless transmission medium, there are instances where the channel used by the access signal 108 can use a wired medium." *Id.* at 7:3–8.

E. Illustrative Claim

Among the challenged claims, claims 1, 9, and 10 are independent claims. Independent claim 1 is directed to a "system for providing secure access to a controlled item." Ex. 1001, 15:42–16:3. Independent claim 9 is directed to a "transmitter sub-system for operating in a system for providing secure access to a controlled item." *Id.* at 16:64–17:18. Independent claim 10 is directed to a "method for providing secure access to a controlled item." *Id.* at 17:19–18:13.

Independent claim 1 is illustrative and is reproduced below.

> 1. A system for providing secure access to a controlled item, the system comprising:
> a database of biometric signatures;
> a transmitter sub-system comprising:
> a biometric sensor for receiving a biometric signal;
> means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and
> means for emitting a secure access signal conveying information dependent upon said accessibility attribute; and
> a receiver sub-system comprising:
> means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said information,

wherein the transmitter sub-system further comprises means for populating the data base of biometric signatures, the population means comprising:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for populating the data base according to the instruction,

wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

Ex. 1001, 15:42–16:3.[6]

F. Prior Art and Asserted Grounds

Petitioner asserts that the challenged claims are unpatentable on the following ground:

[6] Petitioner provides a Claim Listing Appendix as part of the Petition. Pet. 74–77. This Appendix includes all the challenged claims identified by individual clause, such as, for claim 1, labeling the clauses 1(a), 1(b), 1(b)(1), etc. Petitioner refers to these clause labels in its analysis.

Claim(s) Challenged	35 U.S.C. §[7]	Reference(s)/Basis
1, 3–7, 9–11, 13	103(a)	Mathiassen,[8] McKeeth,[9] Anderson[10]

Petitioner also relies on the declaration testimony of Andrew Sears, Ph.D. *See* Ex. 1003;[11] *see also* Ex. 1090 (Dr. Sears' Supplemental Declaration.

II. ANALYSIS

A. Legal Standards

1. Obviousness

Section 103 forbids issuance of a patent when "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

[7] The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284, 296–07 (2011), took effect on September 16, 2011. The changes to 35 U.S.C. §§ 102 and 103 in the AIA do not apply to any patent application filed before March 16, 2013. Because the application for the patent at issue in this proceeding has an effective filing date before March 16, 2013, we refer to the pre-AIA version of the statute.
[8] Mathiassen et al, US 2004/0123113 A1, published June 24, 2004 (Ex. 1004, "Mathiassen").
[9] McKeeth, US 6,766,456 B1, issued July 20, 2004 (Ex. 1005, "McKeeth").
[10] Anderson, US 6,509,847 B1, issued Jan. 21, 2003 (Ex. 1006, "Anderson").
[11] Exhibit 1003 is a 238 page declaration from Dr. Sears, including its Appendix A, which is a detailed mapping of the disclosures of the three applied references to the challenged claims. Dr. Sears currently is a Professor and Dean of the College of Information Sciences and Technology at The Pennsylvania State University. Ex. 1003 ¶ 5. Dr. Sears earned a Bachelor of Science degree in Computer Science, and a Ph.D. degree, also in Computer Science. *Id.* ¶ 6. He has held various positions in academia, including serving as the Interim Chief Information Security Officer at Penn State. *Id.* ¶¶ 7, 8. He has authored or edited a number of computer-related publications and held leadership positions in several computer industry organizations.

invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when available, evidence such as commercial success, long felt but unsolved needs, and failure of others. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966); *see KSR*, 550 U.S. at 407 ("While the sequence of these questions might be reordered in any particular case, the [*Graham*] factors continue to define the inquiry that controls."). The Court in *Graham* explained that these factual inquiries promote "uniformity and definiteness," for "[w]hat is obvious is not a question upon which there is likely to be uniformity of thought in every given factual context." 383 U.S. at 18.

The Supreme Court made clear that we apply "an expansive and flexible approach" to the question of obviousness. *KSR*, 550 U.S. at 415. Whether a patent claiming the combination of prior art elements would have been obvious is determined by whether the improvement is more than the predictable use of prior art elements according to their established functions. *Id.* at 417. To support this conclusion, however, it is not enough to show merely that the prior art includes separate references covering each separate limitation in a challenged claim. *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011). Rather, obviousness additionally requires that a person of ordinary skill at the time of the invention "would have selected and combined those prior art elements in the normal course of research and development to yield the claimed invention." *Id.*

In determining whether there would have been a motivation to combine prior art references to arrive at the claimed invention, it is insufficient to simply conclude the combination would have been obvious without identifying any reason *why* a person of skill in the art would have made the combination. *Metalcraft of Mayville, Inc. v. Toro Co.*, 848 F.3d 1358, 1366 (Fed. Cir. 2017).

Moreover, in determining the differences between the prior art and the claims, the question under 35 U.S.C. § 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. *Litton Indus. Prods., Inc. v. Solid State Sys. Corp.*, 755 F.2d 158, 164 (Fed. Cir. 1985) ("It is elementary that the claimed invention must be considered as a whole in deciding the question of obviousness."); *see also Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1537 (Fed. Cir. 1983) ("[T]he question under 35 U.S.C. § 103 is not whether the differences *themselves* would have been obvious. Consideration of differences, like each of the findings set forth in *Graham*, is but an aid in reaching the ultimate determination of whether the claimed invention *as a whole* would have been obvious.").

As a factfinder, we also must be aware "of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning." *KSR*, 550 U.S. at 421.

Applying these general principles, we consider the evidence and arguments of the parties.

B. Level of Ordinary Skill in the Art

The level of skill in the art is "a prism or lens" through which we view the prior art and the claimed invention. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). "This reference point prevents . . . factfinders

from using their own insight or, worse yet, hindsight, to gauge obviousness." *Id.*

Factors pertinent to a determination of the level of ordinary skill in the art include: (1) educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology; and (6) educational level of workers active in the field. *Env't Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696–697 (Fed. Cir. 1983) (citing *Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.*, 707 F.2d 1376, 1381–82 (Fed. Cir. 1983)). Not all such factors may be present in every case, and one or more of these or other factors may predominate in a particular case. *Id.* Moreover, these factors are not exhaustive but are merely a guide to determining the level of ordinary skill in the art. *Daiichi Sankyo Co. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007). In determining a level of ordinary skill, we also may look to the prior art, which may reflect an appropriate skill level. *Okajima*, 261 F.3d at 1355.

"The *Graham* analysis includes a factual determination of the level of ordinary skill in the art. Without that information, a district court [or an administrative Board] cannot properly assess obviousness because the critical question is whether a claimed invention would have been obvious at the time it was made to one with ordinary skill in the art." *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986); *see also Ruiz v. A.B. Chance*, 234 F.3d 654, 666 (Fed. Cir. 2000) ("The determination of the level of skill in the art is an integral part of the *Graham* analysis.").

Petitioner asserts that a person of ordinary skill in the art would have had "at least a bachelor's degree in computer engineering, computer science,

electrical engineering, or a related field, with at least one year experience in the field of human-machine interfaces and device access security." Pet. 3 (citing Ex. 1003 ¶¶ 35–38). Petitioner also states that "[a]dditional education or experience may substitute for the above requirements." *Id.*

In forming an opinion on the level of ordinary skill applicable to this proceeding, Dr. Sears testifies that he considered various factors, including the type of problems encountered in the art, the solutions to those problems, the rapidity with which innovations are made in the field, the sophistication of the technology, and the education level of active workers in the field. Ex, 1003 ¶ 35. Dr. Sears also testifies that he "placed myself back in the time frame of the claimed invention and considered the colleagues with whom I had worked at that time." *Id.* Dr. Sears opines that a person of ordinary skill would have had the education and experience adopted by Petitioner. *Id.* at ¶ 36.

Patent Owner states it "does not dispute [Petitioner's] characterization" of the level of ordinary skill in the art *See* PO Resp. 5–6.

Based on the prior art, the sophistication of the technology at issue, and Dr. Sears' Declaration testimony, we adopt, with minor modification, Petitioner's undisputed definition of the level of ordinary skill. We determine that in this proceeding a person of ordinary skill would have had a bachelor's degree in computer engineering, computer science, electrical engineering, or a related field, with one year of experience in the field of human-machine interfaces and device access security, or an equivalent balance of education and work experience. We have eliminated the open-ended phrase of "at least" in describing the education and experience of a person of ordinary skill. This open-ended description fails to provide the specificity necessary to define the level of ordinary skill.

C. Claim Construction

We construe each claim "using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b)." 37 C.F.R. § 42.100(b) (2021). Under this standard, claim terms are generally given their ordinary and customary meaning as would have been understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005) (en banc) ("We have frequently stated that the words of a claim 'are generally given their ordinary and customary meaning.'" (citations omitted)).

The challenged claims make extensive use of "means-plus-function" claiming. *See* 35 U.S.C. § 112, ¶ 6 (we cite to the pre-AIA version of the statute applicable to the challenged claims). Means-plus-function claiming occurs when a claim term is drafted in a manner that invokes 35 U.S.C. § 112, ¶ 6, which states:

> An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

See 35 U.S.C. § 112, ¶ 6. *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1347 (Fed. Cir. 2015) (en banc).

Independent claim 1, for example, includes numerous means-plus-function clauses: *See, e.g.*, Ex. 1001, 15:47–52, 54–67. Independent claim 9 also uses numerous means-plus-function clauses. *Id.* at 17:1–15. On the record before us, we have not been directed to any dispute between the

parties as to whether § 112, ¶ 6 applies to numerous clauses in the challenged claims.

Where claim language may be construed according to 35 U.S.C. § 112(f) (or its predecessor, § 112, ¶ 6), a petitioner must provide a construction that includes both the claimed function and the specific portions of the specification that describe the structure, material, or acts corresponding to each claimed function. 37 C.F.R. § 42.104(b)(3).

In accordance with these requirements, Petitioner provides specific constructions for all the means-plus-function clauses in the challenged claims. Pet. 6–9. Petitioner asserts its proposed constructions are consistent with constructions made by the Texas district court in the related litigation between the parties (*see* Ex. 1077), constructions agreed to by the parties in the related litigation (*see* Ex. 1079), or constructions proposed by Patent Owner in the related litigation (*see* Ex. 1073). [12]

Patent Owner does not dispute any of the myriad means-plus-function clauses construed by Petitioner. *See* Response; Sur-reply.

Thus, we adopt Petitioner's undisputed findings and conclusions for these means-plus-function terms as our own, and repeat them below for convenient reference. *See* Pet. 6–9.

[12] The cited exhibits 1073, 1077, and 1079 are from the case *prior to* its transfer from the Western District of Texas to the Northern District of California.

Claim Term	*Support*	*Structure and Function*
Claims 1, 9: "means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute" **Court Construction, Ex. 1077**	*'208 Patent*, 4:8–13, 4:15–17, 4:40–45, 4:47–49, 5:50–67, 6:56–7:2, 7:65–8:10, 8:67–9:5, 14:10–42, Fig. 2, items 103, 105, Fig. 3, item 202, (Ex. 1077, 4)	Structure: database and computer program product having a computer readable medium having a computer program recorded therein, with code for Function: matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute
Claim 10: "means for emitting a secure access signal capable of granting more than two types of access to the controlled item" **CPC Construction, Ex. 1073**	*'208 Patent*, 4:8–13, 4:18–22, 4:40–45, 4:50–54, 8:17–28, 10:24–44 (Ex. 1073, 7)	Structure: computer program product having a computer readable medium having a computer program recorded therein, with code for Function: emitting a secure access signal capable of granting more than two types of access to the controlled item

Claim Term	*Support*	*Structure and Function*
Claims 1, 9: "means for emitting a secure access signal conveying said informationdependent upon said accessibility attribute" **CPC Construction, Ex. 1073**	*'208 Patent*, 4:8–13, 4:18–22, 4:40–45, 4:50–54, 5:65–6:6, 6:28–55, 8:19–35, 14:16–20 (Ex. 1073, 4).	Structure: computer program product having a computer readable medium having a computer program recorded therein, with code for Function: emitting a secure access signal conveying said information dependent upon said accessibility attribute
Claims 1, 10: "means for receiving the transmitted secure access signal" **Agreed-Upon Construction, Ex. 1079**	*'208 Patent,* 6:16–19, FIGs. 2, 4, 10 (Ex. 1079) * Note the Parties' communications in the district court correspondence did not identify specification support	Structure: receiver 118 Function: receiving the transmitted secure access signal
Claims 1, 10: "means for providing conditional access to the controlled item dependent upon [said] information [in said secure access signal]" **Agreed-Upon Construction, Ex. 1079**	*'208 Patent,* 8:65–9:15, 8:17–35, 11:27–12:38, FIGs. 2, 4, 7, 10 (Ex. 1079) * Note the Parties' communications in the district court correspondence did not identify specification support	Structure: controller 109 executing software 304 Function: providing conditional access to the controlled item dependent upon information in said secure access signal

Claim Term	*Support*	*Structure and Function*
Claims 1, 9: "means for receiving a series of entries of the biometric signal" **CPC Construction, Ex. 1079**	*'208 Patent,* 4:8–14, 4:25–34, 4:40–46, 5:53–59, 7:66–8:6, 10:45–63, 12:55–59 (Ex. 1073, 4–5)	Structure: computer program product having a computer readable medium having a computer program recorded therein, with code for Function: receiving a series of entries of the biometric signal
Claims 1, 9: "means for mapping said series into an instruction" **Court Construction, Ex. 1077**	*'208 Patent,* 4:25–31, 4:37, 5:50–6:27, 10:45–11:2, 12:55–59, 12:67–13:3, Fig. 2, items 103, 107, 121 (Ex. 1077, 3)	Structure: computer program product having a computer readable medium having a computer program recorded therein, with code for Function: mapping said series into an instruction
Claims 1, 9: "means for populating the database according to the instruction" **Court Construction, Ex. 1077**	*'208 Patent,* 4:25–31, 4:38–39, 10:57–11:2, 12:43–45, 13:9–11, 13:15–19 (Ex. 1077, 3)	Structure: database and computer program product having a computer readable medium having a computer program recorded therein, with code for Function: populating the database according to the instruction

Claim Term	*Support*	*Structure and Function*
Claims 1, 9: "means for populating the data base of biometric signatures" **Court Construction, Ex. 1077**	*'208 Patent*, 4:25–31, 4:38–39, 10:32–34, 10:57–11:2, 12:43–45, 13:9–1, 13:15–19 (Ex. 1077, 3–4)	Structure: database and computer program product having a computer readable medium having a computer program recorded therein, with code for Function: populating the data base of biometric signatures

Concerning claim terms that are *not* in means-plus-function format, Petitioner also proposes constructions for the claim terms "database," "conditional access," "biometric signal," and "accessibility attribute." Pet. 9. Petitioner asserts the proposed constructions are either agreed to by the parties (*see* Ex. 1079) or made by the district court (*see* Ex. 1077).

Patent Owner proposes "constructions" (1) for the term "accessibility attribute" (Resp. 6–7); (2) the phrase requiring a series of entries of the biometric signal "characterised according to at least one of the number of said entries and a duration of each said entry" (*id*. at 7–11); and (3) the "populate" the database limitation concerning enrolling or authorizing new users (*id.* at 11–12).

"[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'" *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Ltd.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). Here, we determine the claim terms that need specific

construction are the three terms proposed by Patent Owner for specific construction. Accordingly, we construe these terms below.

1. General Claim Construction Principles

"It is a 'bedrock principle' of patent law that 'the claims of a patent define the invention to which the patentee is entitled the right to exclude.'" *Phillips*, 415 F.3d at 1312 (citations omitted). "[T]here is no magic formula or catechism for conducting claim construction." *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 801, 809 (Fed. Cir. 2021) (quoting *Phillips*, 415 F.3d at 1324). Fortunately, however, there is substantial judicial guidance.

Claim construction requires determining how a skilled artisan would understand a claim term "in the context of the entire patent, including the specification." *Grace Instrument Indus., LLC v. Chandler Instruments Co., LLC*, 57 F.4th 1001, 1008 (Fed. Cir. 2023) (quoting *Phillips*, 415 F.3d at 1313. *Id.* (citation omitted). "[C]laims must be read in view of the specification, of which they are a part." *Id.* (quoting *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 978 (Fed. Cir. 1995) (en banc)). The Specification, or more precisely, the written description, is the "single best guide to the meaning of a disputed term." *Id.* (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996), and "is, thus, the primary basis for construing the claims." *Id.* (citation omitted). Although claim terms are interpreted in the context of the entire patent, it is improper to import limitations from the Specification into the claims. *Phillips*, 415 F.3d at 1323. Thus, we are careful not to cross that "fine line" that exists between properly construing a claim in light of the specification and improperly importing into the claim a limitation from the specification." *Comark Commc'ns., Inc. v. Harris Corp.*, 156 F.3d 1182, 1186 (Fed. Cir. 1998) ("We recognize that there is sometimes a fine line between reading a

claim in light of the specification, and reading a limitation into the claim from the specification.").

While certain terms may be at the center of the claim construction debate, the context of the surrounding words of the claim also must be considered in determining the ordinary and customary meaning of those terms. *ACTV, Inc. v. Walt Disney Co.*, 346 F.3d 1082, 1088 (Fed. Cir. 2003).

We also consider the patent's prosecution history. *Phillips, 415 F.3d* at 1317.

In construing the claims, we may also look to available "extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art." *Phillips*, 415 F.3d at 1314 (quoting *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1116 (Fed. Cir. 2004)).

2. "Accessibility Attribute"

In our Decision to Institute this proceeding, we adopted, for purposes of that Decision, Petitioner's unopposed asserted claim construction for "accessibility attribute," which was an "attribute that establishes whether and under which conditions access to the controlled item should be granted." Dec. Inst. 13 (citing Pet. 9 (citing the Texas District Court's claim construction, Ex. 1077, 2–3)). We note here that the District Court included the phrase "to a user" at the end of the construed term, which Petitioner did *not* include. The complete construction by the District Court is an "attribute that establishes whether and under which conditions access to the controlled item should be granted *to a user*." Ex. 1077, 2 (emphasis added). The District Court did not cite any intrinsic or extrinsic evidence to support its construction.

In Patent Owner's Response, Patent Owner acknowledges Petitioner's proposed construction but asserts that "a mere binary decision to grant access to a device does not constitute an 'accessibility attribute.'" PO Resp. 6–7; *see also* Ex,2011 ¶ 45 (Patent Owner's expert, Dr. Easttom,[13] testimony that the construction of the term "accessibility attribute" in our Decision to Institute this proceeding "requires more than the binary determination of whether to grant access to a controlled item by virtue of the 'under which conditions' language"). Patent Owner also asserts that Petitioner's "position on the 'accessibility attribute' limitation is muddied at best." *Id.* at 12. According to Patent Owner, Petitioner "and its expert appear to argue that 'accessibility attribute' can be a binary access decision." *Id.* at 13 (citing Paper [Pet.] 1 at 42–44).

Thus, Patent Owner asserts what an "accessibility attribute" is not (it is not a binary decision), but fails to assert a construction of what an "accessibility attribute" is.

We do *not* understand Petitioner to be asserting a construction of the term "accessibility attribute" to mean simply a "binary decision" to grant or not grant access to a locked structure or device. Nor, did our Decision to Institute adopt such a "binary decision." The construction asserted by

[13] Exhibit 2011 is a 36-page declaration from Dr. Easttom. Dr. Easttom earned a D.Sc. degree in Cyber Security, a Ph.D. degree in Technology, and three master's degrees (one in Applied Computer Science, one in Education, and one in Systems Engineering). Ex. 2011 ¶ 7. Dr. Easttom testifies that he has 30 years of experience in the computer science industry including extensive experience with computer security, computer software, and computer networking; that he has authored 37 computer science books; that he has authored over 70 research papers; and that he is an inventor with 25 patents, including patents related to computer networking. His CV (Ex. 2012) provides details of his extensive experience and education.

Petitioner in this proceeding, and the construction adopted in our Decision to Institute this proceeding requires "an attribute that establishes *whether and under which conditions* access to the controlled item should be granted." Dec. Inst. 13 (citing Pet. 9 (citing the Texas District Court's claim construction, Ex. 1077, 2–3) (emphasis added)).

As we explain in our analysis below, to avoid any confusion of the meaning of "accessibility attribute," we clarify the construction to add the phrase "if any" to modify the "conditions" that may, or may not, be imposed to allow access. Thus, we determine that an "accessibility attribute" is "an attribute that establishes whether and under which conditions, if any, access to the controlled item should be granted." Based on the language of the claims and Specification, the "accessibility attribute" may include only an "access attribute," which is "unconditional." *See* Ex, 1001, 8:19–25 (stating "the accessibility attribute may comprise one or more of an access attribute (granting unconditional access) . . .), 16:13–23 (claim 3 requiring "at least one of" an access attribute, a duress attribute, and an alert attribute).[14]

Notwithstanding Patent Owner's Response, Petitioner asserts that "[t]he Parties agree to apply the District Court's construction for the claimed "accessibility attribute." Reply 1. Petitioner also states, however, that Petitioner is relying on McKeeth for teaching two accessibility attributes (duress and alert) even though "the '208 Patent's independent claims only require outputting a single accessibility attribute." *Id.* at 2.

Petitioner clarifies its position on the construction of "accessibility attribute" by further explaining Petitioner's view that "the '208 Patent

[14] To avoid any confusion, we note that an "access attribute" is one specific example of the generic term "accessibility attribute." Ex. 1001, 8:19–25.

describes outputting an accessibility attribute that includes 'access' without any conditions, which satisfies the under which conditions' construction component." Reply. 4.

We begin our claim construction analysis with the language used in the claims.

a) Claims

The term "accessibility attribute" appears in all the challenged claims.

Independent claim 1 includes the following two clauses that refer to an "accessibility attribute": (1) "means for matching the biometric signal against members of the database of biometric signatures *to thereby output an accessibility attribute*" (Ex. 1001, 15:47–49)[15]; and (2) "means for *emitting a secure access signal conveying information dependent upon said accessibility attribute*" (*id*. at 15:50–52). These two references merely establish that an "accessibility attribute" is an output access signal based on matching the biometric signal against the authorized user database of biometric signatures. *See id.* at 5:61–65 ("Thus for example if the request 102 is the thumb press on the biometric sensor panel 121 then the user database 105 contains biometric signatures for authorised [sic] users against which the request 102 can be authenticated.").

These clauses provide no further structure or function of the claimed "accessibility attribute."

Claim 1 also includes a clause stating that "conditional access" to a user is "dependent upon" information in the "accessibility attribute." *Id.* at 15:56–57. This clause does not require or state that there is, or is not, conditional access. It merely states that "conditional access," if any,

[15] All italicized emphasis of claim language has been added.

depends on what information is in the "accessibility attribute." *See id.* at 15:50–52 (stating that the "information" in the "access signal" in claim 1 is "dependent upon" the "accessibility attribute"). Thus, based on the claim language in claim 1, the scope of the "accessibility attribute" is undefined. The only requirement is that it provide access for authorized users.

Claim 3, dependent on claim 1, states that "the [authorized user] database of biometric signatures comprises signatures in *at least one of* a system administrator class, a system user class, and a duress class." Ex. 1001, 16:13–16 (emphasis added). Thus, consistent with Petitioner's argument summarized above (*see* Reply 4–5), the system administrator may be the only authorized user in the database. Claim 3 also further defines the "accessibility attribute" as comprising:

> *an access attribute* if the biometric signal matches a member of the database of biometric signatures;
>
> *a duress attribute* if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and
>
> *an alert attribute* if the biometric signal does not match a member of the database of biometric signatures.

Id. at 16:18–24 (emphasis added).

In claim 3, the conditional "duress attribute" applies only if the user is a member of the "duress class" in the database of biometric signatures. There is, however, no requirement that any member of the "duress class" be in the database.

We recognize that the Federal Circuit has held that the plain and ordinary meaning of "at least one of" is "one or more," but that when the phrase is used in a claim, the issue is what "at least one of" is used to

modify. *See SuperGuide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 886 (Fed. Cir. 2004). In *SuperGuide*, the court held that, when "[t]he phrase 'at least one of' precedes a series of categories of criteria, and the patentee used the term 'and' to separate the categories of criteria," the phrase connotes a conjunctive list and requires selecting at least one value for each category. *Id.* For example, in *SuperGuide*, the claim phrase "storing at least one of a desired program start time, a desired program end time, a desired program service, and a desired program type" was interpreted as requiring storing at least one desired program start time, at least one desired program end time, and so forth. *Id.* at 884.

Courts have not, however, interpreted *SuperGuide* as setting forth a *per se* rule that the use of "at least one of" followed by "and" necessarily connotes a conjunctive list. *See Fujifilm Corp. v. Motorola Mobility LLC*, Case No. 12–CV–03587–WHO, 2015 WL 1265009, at *8 (N.D. Cal. Mar. 19, 2015) (summarizing cases and noting that "*SuperGuide* did not erect a universal rule of construction for all uses of 'at least one of' in all patents"). In particular, courts have found *SuperGuide* inapplicable when the listed items following "at least one of" are not categories containing many possible values. *See id.*; *see also TQ Delta, LLC v. Comcast Cable Commc'ns, LLC*, No. 1:15–CV–00611–RGA, 2016 WL 7013481, at *8 (D. Del. Nov. 30, 2016) (list following "at least one of" was of parameters to be selected from, not categories). The Board has also distinguished *SuperGuide* on this basis. *See Hewlett–Packard Co. v. MPHJ Tech. Invs., LLC*, Case IPR2013–00309, Paper 9, slip op. at 8 (PTAB Nov. 21, 2013); *Daifuku Co., Ltd. v. Murata Machinery, Ltd.*, Case IPR2015–00083, Paper 63, slip op. at 4–5 (PTAB May 3, 2016); *Apple, Inc. v. Evolved Wireless LLC*, No. IPR2016-01177, 2017 WL 6543970, at *4 (P.T.A.B. Dec. 20, 2017).

Relevant to our inquiry, therefore, is whether the items that follow "at least one of" in the challenged claims of the '208 patent are categories that may have multiple values (such as in *SuperGuide*) or individual parameters having only one value. Here, we think it is clear that the accessibility attributes and the classes of users are individual parameters that apply to individual people.

As noted above, the first user of the disclosed and claimed invention "is automatically categorised as an administrator." Ex. 1001, 10:28–32. This first user may be the only authorized user. Thus, the only database entry for this first user is a "system administrator class" entry that will generate only an "access attribute (granting *unconditional* access)." *Id.* at 8:19–21 (emphasis added). This is not unlikely because the claims are specifically limited to a "controlled item" that is either "a locking mechanism of a physical access structure," or "an electronic lock on an electronic computing device." *See, e.g.*, Ex. 1002, 336 (Examiner's amendment to application claim 69, which became patent claim 1 (*id.* 355, Index of Claims). A similar Examiner's Amendment was entered in each independent claim. *See id.* at 338–339 (amending application claims 78, 79, which became patent claims 9 and 10). The owner of an individual computing device may be the only authorized user of that device.

Claim 3 allows a database of only a first and only user, who is automatically the system administrator. Ex. 1001, 16:13–16. ("the database of biometric signatures comprises signatures in *at least one of* a system administrator class, a system user class, and a duress class" (emphasis added)). There may be no other individuals in the "system user class" or the "duress class."

Additionally, dependent claim 3 further limits claim 1 by stating the "accessibility attribute" in claim 1 "preferably" comprises[16] the three specific attributes stated in claim 3 – "an "access attribute"; "a duress attribute"; and "an alert attribute." This listing in claim 3 establishes a presumption that these three requirements are *not* included in the claimed "accessibility attribute" in claim 1. *Phillips*, 415 F.3d at 1314–15 ("Differences among claims can also be a useful guide in understanding the meaning of particular claim terms. For example, the presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim." (citations omitted)).[17]

---

[16] "[I]n general, a patent claim reciting an apparatus "comprising" various components merely means that the apparatus "includ[es] but is not limited to" those components. *Rothschild Connected Devices Innovations, LLC v. Coca-Cola Co.*, 813 F. App'x 557, 562 (Fed. Cir. 2020) (nonprecedential) (citations omitted).

[17] We recognize that the Board "must base its decision on arguments that were advanced by a party, and to which the opposing party was given a chance to respond." *Masimo Corp. v. Apple Inc.*, Nos. 2022-1631 *et al*, slip op. at 8 (Fed. Cir. Sep. 12, 2023 (nonprecedential)) (citing *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016). The parties argued claim construction, but did not discuss specifically claim differentiation as part of their claim construction analysis. Petitioner argued, however, that the claims allowed for "administrator access as an exemplary access without conditions." Reply 4–5. Patent Owner addressed this in its Sur-reply. Sur-reply 22. Our claim construction analysis, as stated in the text, follows controlling procedures from *Phillips*. The parties also were advised that:

> claim construction, in general, is an issue to be addressed at trial. Claim construction will be determined at the close of all the evidence and after any hearing. The parties are expected to assert all their claim construction arguments and evidence in the Petition, Patent Owner's Response, or otherwise during trial, as permitted by our rules.

Claim 5, dependent on claim 1, specifies the claimed system "comprises" conditional approval or denial of access based on "*one of*" three specific types of the "accessibility attribute" stated in claim 3 – "an access attribute;" "a duress attribute;" and "an alert attribute." Thus, a system with only an "access attribute" type of "accessibility attribute" satisfies the requirement of claim 5 for only "one of" the three types of attributes. The access attribute merely provides access, without any conditions if the user's biometric signal is in the database. No conditional "duress attribute;" or "alert attribute" is required in claim 5.

Independent claim 9, directed to a "transmitter sub-system" includes the same two clauses as in claim 1 concerning the "accessibility attribute."

Independent claim 10, directed to a "method for providing secure access" also includes the same two clauses as in claim 1 concerning the "accessibility attribute." Method claim 10, however, states the verb form of "matching" and "emitting" rather than the patent law "means-plus-function form in system claim 1 of "means for matching" and "means for emitting."

Based on the claim language, the doctrine of claim differentiation, and the analysis above, we determine that an "accessibility attribute," as used in claims 1, 9, and 10, means that a user with a biometric signature in the database is given access to the controlled item. As used in the independent claims, there are no other conditions imposed.

For dependent claims 3 and 5, however, the "accessibility attribute" may also include a "duress attribute" and/or an "alert attribute."

Dec. Inst. 14.

Thus, based on the claim language, an "accessibility attribute" is an attribute that establishes whether and under which conditions, if any, access to the controlled item should be granted.

b) Specification

Claims "must be read in view of the specification, of which they are a part." *Phillips*, 415 F.3d at 1315 (citation omitted). "The specification "is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term." *Id.* (citation omitted). Thus, we turn to the Specification for additional guidance on the meaning of the claim term "accessibility attribute."

The Specification states that the "accessibility attribute establishes whether and under which conditions access to the controlled item 111 should be granted to a user." Ex. 1001, 8:17–19. This is the construction adopted in our Decision to Institute this proceeding,

The Specification further states:

> the accessibility attribute may comprise *one or more of* an *access attribute (granting unconditional access)*, a *duress attribute* (granting access but with activation of an alert tone to advise authorities of the duress situation), an *alert attribute* (sounding a chime indicating that an unauthorised [sic], but not necessarily hostile, person is seeking access, and a *telemetry attribute*, which represents a communication channel for communicating state information for the transmitter sub-system to the receiver sub-system such as a "low battery" condition.

Id. at 8:19–28 (emphases added). Thus, while four different accessibility attributes are disclosed (access attribute, duress attribute, alert attribute, and telemetry attribute), the Specification, consistent with the claims discussed above, states that the disclosed invention "may comprise *one or more of"*

these four attributes. Ex. 1001, 8:20. The Specification also states that an "access attribute" grants "unconditional access." *Id.* at 8:20–21.

The term "accessibility attribute" does not appear in the Specification after column 8 until it appears again in the claims.

Thus, based on the Specification, an "accessibility attribute" is an attribute that establishes whether and under which conditions, if any, access to the controlled item should be granted. The term "if any" is required because an "access attribute" grants "unconditional access" (*id.*) and it may be the only attribute included as an "accessibility attribute." *See id.* at 8:19–25 (stating the accessibility attribute "may comprise one or more of" the four disclosed specific attributes).

c) Prosecution History

The parties have not directed us to any persuasive evidence from the proceedings leading to issuance of the '208 patent to inform our construction of the term "accessibility attribute."

We note that in its final amendment and response prior to allowance of the application that matured into the '208 patent, the applicant characterized the "claimed invention" as "matching a received biometric signal against members of a database of biometric signatures." Ex. 1002, 297. Applicant also asserted that "new [application] claim 69 [patent claim 1] is not directed towards performing a simple biometric authentication, but rather is directed towards using biometric authentication to either produce or prevent physical access to a controlled item." *Id.* at 300. Thus, the claim uses a biometric authentication to produce a result, which is whether, and under what conditions, if any, access to a controlled item will be permitted. We also note that applicant's argument that "using biometric authentication

to either produce or prevent physical access to a controlled item" (*id.*) is a binary determination concerning access.

The Examiner entered the following statement under the heading "EXAMINER'S STATEMENT OF REASONS FOR ALLOWANCE"

> Regarding the claimed terms, the Examiner notes that a 'general term must be understood in the context in which the inventor presents it.' In re Glaug 283 F.3d 1335, 1340, 62 USPQ2d 1151, 1154 (Fed. Cir. 2002) [sic]. Therefore the Examiner must interpret the claimed terms as found on the specification of the instant application. Clearly almost all the general terms in the claims may have multiple meanings. So where a claim term 'is susceptible to various meanings, . . . the inventor's lexicography must prevail. . . . ' Id. [sic] Using these definitions for the claims, the claimed invention was not reasonably found in the prior art.
>
> This communication warrants No Examiner's Reason for Allowance, Applicant's reply make[s] evident the reasons for allowance, satisfying the 'record as a whole' proviso of the rule 37 CFR 1.104(e). Specifically, amended independent claims 69, 78, and 79 in view of examiner's amendment and the substance of applicant's persuasive arguments, see pp. 11-16 in remarks filed 07/27/2015 from the record and no statement is deemed necessary (see MPEP 1302.14).
>
> None of the prior art of record taken by itself or in any combination, would have anticipated or made obvious the claimed invention of the present application at or before the time it was filed.

Ex. 1002, 323–324.

d) Extrinsic Evidence

The parties do not direct us to any persuasive extrinsic evidence concerning the meaning of the term "accessibility attribute."

e) Claim Construction Conclusion for "Accessibility Attribute"

We recognize that "[t]he very nature of words would make a clear and unambiguous claim a rare occurrence." *Autogiro Co. of Am. v. United States*, 384 F.2d 391, 396 (Ct. Cl. 1967). The Federal Circuit, however, has provided a beacon, which we have followed, to guide us in determining the proper construction when we encounter ambiguities or differing interpretations from the parties:

> Ultimately, the interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim. The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction.

Renishaw PLC v. Marposs Societa' per Azioni, 158 F.3d 1243, 1250 (Fed. Cir. 1998) (citations omitted).

Based on the evidence and the analysis above, we determine that that the term "accessibility attribute" means "an attribute that establishes whether and under which conditions, if any, access to the controlled item should be granted." This is the construction that stays true to the claim language and most naturally aligns with the patent's description of the invention.

3. Biometric Signal Characterised by Number and Duration

All of the challenged claims include a clause that requires "receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry." *See* Ex. 1001, 15:61–64 (for independent claim 1), 17:9–12 (for independent claim 9), 17:30–32 (for independent claim 10). In claims 1 and 9, this clause is expressed in a "means-plus-function" format. In claim 10,

this clause is expressed as the method steps of "receiving" entries of biometric signals and "determining" at least one of the number of entries and a duration of each entry. We refer to these clauses collectively as the "number and duration" clauses.

These number and duration clauses all go to the embodiment of the invention that allows the administrator to require a biometric input signal that comprises "either or both (a) the number of finger presses and (b) the relative duration of the finger presses." *Id.* at 10:49–52 (This is the "dit, dit, dit, dah" form of biometric signal discussed in the Specification (*id.* at 10:57–63) and discussed above in this Decision.). The capability for an administrator to use this disclosed embodiment exists in the claimed system and method whether the administrator chooses to use it or not. As stated in the Specification, the administrator may use a single thumb press on a sensor for the required biometric signal. *Id.* at 5:56–59 ("for example, if the biometric sensor 121 in the code entry module 103 is a fingerprint sensor, then the request 102 typically takes the form of a thumb press on a sensor panel"). Alternatively, the administrator "can provide control information to the code entry module by providing a succession of finger presses to the biometric sensor 121." Ex. 1001, 10:5–7. Thus, whether using a single thumb press or a succession of finger presses of variable number and duration, the input vehicle is the same – biometric sensor 121.

Patent Owner asserts that Petitioner, and the Board in its Decision to Institute this proceeding, improperly "blur the lines" between "'knowledge-based' security features (those based on knowledge, such as a passcode or particular pattern, and not on any attribute of the user), and a biometric signal based on the unlearnable attribute of the user." PO Resp. 9. We

disagree. Patent Owner fails to properly understand Petitioner's, and our, analysis of the number and duration clauses.

Patent Owner asserts:

> Crucially, the antecedent for this series is 'a series of entries of the biometric signal,' *i.e.*, the entries and corresponding series are 'of the biometric signal,' and the 'number of said entries and a duration of each said entry' refers to the entries of the biometric signal, and not an entry of some other information, such as knowledge-based information.

Id. at 9–10. As explained above, in our Decision to Institute, and in this Decision, we construe the number and duration clauses to require a number and duration of biometric signals because the input for these biometric signals is a biometric sensor, as disclosed in the Specification. A fingerprint sensor's ability to recognize a fingerprint is not turned off when a succession of finger presses is applied to the fingerprint sensor. Thus, contrary to Patent Owner's argument (*see* PO Resp. 11), our construction of the number and duration clauses is not based on a "knowledge-based security feature."

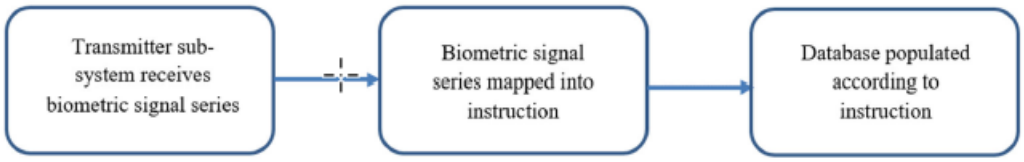
In summary, our construction of the number and duration clauses is that the number and/or duration of entries is based on entries of a biometric signal, such as a finger press on a fingerprint sensor. Based on the claim language and the Specification (*see* Ex. 1001, 10:50–52 ("the control information is encoded by either or both (a) the number of finger presses and (b) the relative duration of the finger presses"), this is the construction that stays true to the claim language and most naturally aligns with the patent's description of the invention.

4. Populate the Database

Patent Owner asserts that if and when the number and duration clause (citing clause 1(d)(1) in Petitioner's Claim Listing Appendix (Pet. 74)) is

used by an administrator to establish an authorized user, that information is "mapped into an instruction and the resulting instruction is used to populate the database of biometric signatures." PO Resp. 11 (citing representative clauses 1(d)(2) and 1(d)(3) from Petitioner's Claim Listing Appendix). Patent Owner also acknowledges that "the 'populate' limitation in claim 1 is part of that enrolling feature." PO Resp. 11. We understand that reference to the "enrolling" feature is a reference to the administrator establishing a database of authorized users that will be used to match a received biometric signal against members of a database of biometric signatures and provide access to the controlled item dependent upon the success or otherwise of the matching operation. Ex. 1002, 297–298.

Patent Owner asserts that "[t]o satisfy the requirements for antecedent claiming, 'said series' in clause 1(d2) must refer to the 'series of entries of the biometric signal' in clause 1(d1)." PO Resp. 11. Patent Owner provides the following flow diagram for populating the database:



Id. at 12 (citing Ex. 2011 ¶ 82). The flow diagram provides Patent Owner's graphic interpretation of the three steps involved in populating the database of approved users. These basic steps apply whether the biometric signal is a single finger press or a series of finger presses.

In its claim construction arguments, Patent Owner attempts to draw a sharp distinction between a process using a single finger press, and a process that uses the number and duration of finger presses, as two technologically distinct processes. Patent Owner has not, however, cited any persuasive

evidence to support this asserted distinction. In fact, the evidence is to the contrary. As we have noted throughout this claim construction analysis, the controlling case law is consistent in stating that the Specification is the single best guide to the meaning of a disputed term, and is, thus, the primary basis for construing the claims. *E.g.*, *Grace Instrument*, 57 F.4th at 1008. In the '208 patent, the Specification also is consistent in stating that using a number and duration of finger presses as a biometric input signal, and using a single finger press, are done exactly the same way – both use the same biometric fingerprint sensor. *See, e.g.*, Ex. 1001, 10:5–7 (the administrator "can provide control information to the code entry module by providing a succession of finger presses *to the biometric sensor 121*"**)** (emphasis added).

The Specification also is consistent in stating that the system administrator establishes a database of authorized users, or authorized biometric signatures, by using appropriate software to create, or populate, the database. *See, e.g.*, *Id.* at 14:10–20.[18] There is no persuasive evidence to which we have been directed that the biometric fingerprint sensor ceases to function as a biometric fingerprint sensor when the administrator establishes a database using the number and duration of finger presses. Patent Owner's

[18] The cited text from the Specification states:

> FIG. 10 is a schematic block diagram of the system in. FIG. 2. The disclosed secure access methods are preferably practiced using a computer system arrangement 100', such as that shown in FIG. 10 wherein the processes of FIGS. 3-4, and 6-9 may be implemented as software, such as application program modules executing within the computer system 100'. In particular, the method steps for providing secure access are effected by instructions in the software that are carried out under direction of the respective processor modules 107 and 109 in the transmitter and receiver sub-systems 116 and 117.

argument is actually to the contrary in that Patent Owner asserts that the number and duration of finger presses is a biometric signal. PO Resp. 9–10 ("the entries and corresponding series are 'of the biometric signal,' and the 'number of said entries and a duration of each said entry' refers to the entries of the biometric signal, and not an entry of some other information, such as knowledge-based information."). This means the number and duration of entries must include a biometric component.

If the number and duration of presses did not include a biometric component, it would be simply a "knowledge-based" security measure, based on a pattern rather than based on a unique physical attribute of the user. Patent Owner asserts that such a pattern can be learned, and thus is inconsistent with the '208 patent's claims and disclosure. PO Resp. 8–10. Whether the software used by the administrator to populate the database of approved users relies on this biometric component is not disclosed in the '208 Specification.

We now turn to the merits of Petitioner's asserted Grounds of unpatentability.

D. Ground 1
Claims 1, 3–7, 9–11, 13
Based on Mathiassen, McKeeth, and Anderson

Petitioner contends that claims 1, 3–7, 9–11, 13 would have been obvious over the combination of Mathiassen, McKeeth, and Anderson. Pet. 12–63.

1. Mathiassen (Ex. 1004)

We make the following finding of facts concerning Mathiassen.

Rather than using passwords or "tokens," such as an entry card, Mathiassen discloses a portable fob-type fingerprint sensor to access secured

items, such as vehicles, computers, safes, medicine cabinets, and weapons cabinets. Ex. 1004 ¶¶ 1–4, 16–18, 109–113.

Figure 8 from Mathiassen is reproduced below.

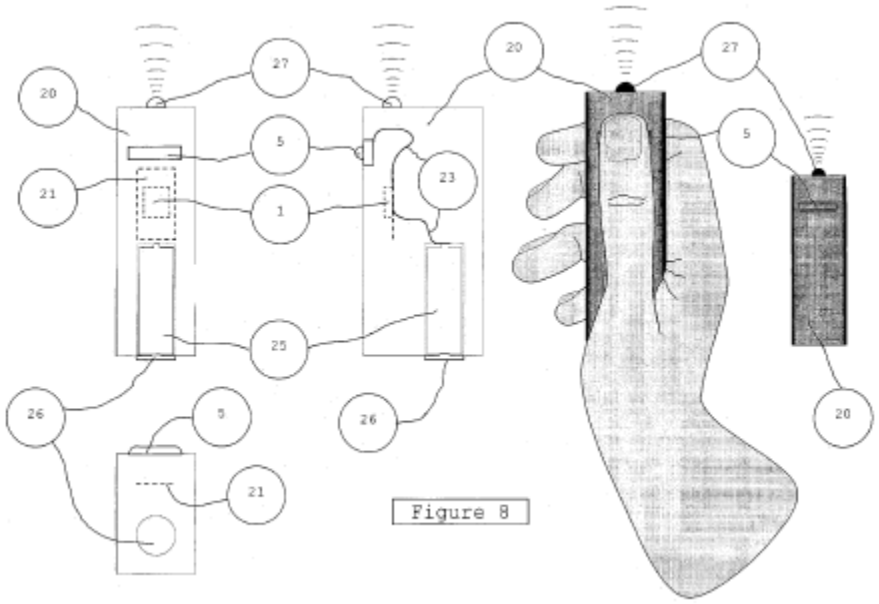


Figure 8 is a schematic illustration of a "user input device" providing access to a vehicle door. As shown in Figure 8, portable device 20 contains fingerprint sensor 5 coupled to a miniature printed circuit board 21 on which is mounted integrated circuit ("IC") 1. Ex. 1004 ¶ 147. Thus, remote control 20 becomes a biometric sensor. *Id.* ¶ 5. Remote biometric control 20 includes battery 25 as a power supply. Ex. 1004 ¶ 147. Battery 25 is connected to printed circuit board ("PCB") 21 by wires. *Id.*

Remote biometric control 20 also is equipped with wireless 2-way transceiver 27. All the active components are connected to integrated circuit 1 by cables 23 through printed circuit board 21. *Id.*

Ignition control device 15 (*see* Fig. 6) is mounted inside the car on gear stick 71 or on steering wheel 72. *Id.* ¶ 148. Remote control 20 and embedded ignition control 15 are both connected to a central computer (not

shown) in the car. *Id.* ¶ 149. Remote control 20 is connected to the central computer by 2-way wireless transceiver 27, while ignition control 15 is hard-wired to the central computer. *Id.*

2. McKeeth (Ex. 1005)

We make the following finding of facts concerning McKeeth.

McKeeth discloses a method and system for authenticating a user to access a computer system. Ex. 1005, Abstr.

McKeeth summarizes the problems with current systems for accessing computers, such as using a private identification code or password (Ex. 1005, 1:14–30),[19] or a machine-readable card (*id.* at 1:31–36). McKeeth also notes that "some computer makers considered using the user's fingerprint to authenticate and grant access to the computer system." *Id.* at 1:36–38. McKeeth recognized, however, that even using fingerprints was not without problems because "a sophisticated computer hacker may be able to copy the user's fingerprint and provide a simulated signal to the computer system to obtain access." *Id.* at 1:51–54.

The method and system disclosed in McKeeth provide for one or more of various types of user inputs to be used, alone or in combination, for authentication. These various inputs can be a password, a unique series of clicks of a mouse, a unique geometric pattern created by the user (*see* Figs. 3A–3D (illustrating a simple triangle, rectangle, line, or circle drawn by the user), an audio sensor (for voice recognition), or an optical scanner for fingerprint, retina scans, or other biometric inputs. Ex. 1005, 2:2:53–3:12.

Figure 1 from McKeeth is reproduced below.

[19] Citations are to column:line of McKeeth.

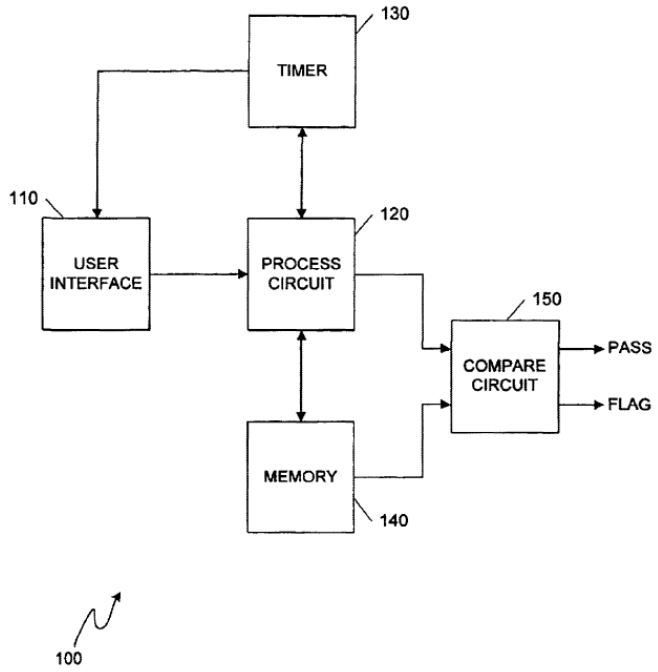


Figure 1 from McKeeth is a block diagram showing one version of the method and system for authenticating the identity of a user disclosed in McKeeth. Ex. 1005, 2:36–37. As shown in Figure 1, computer system 100 includes user interface 110 that is operationally connected to process circuit 120. *Id.* at 2:55–57. User interface 110 may be any input device that is used to enter or communicate information to computer system 100, such as a keyboard, mouse, trackball, pointer, touch-screen, remote terminal, audio sensor, optical scanner, telephone, or any similar user interface. *Id.* at 2:57–61.

Process circuit 120 is configured to receive input signals from user interface 110. The process circuit is operationally connected with timer 130 that measures time duration between the various input signals. Ex. 1005, 3:36–38. If, for example, the user performs a fingerprint scan and/or pattern within the designated time, process circuit 120 communicates the input signals to compare circuit 150 for authentication. *Id.* at 3:52–55. Compare

circuit 150 is operationally coupled to memory 140, which stores a list of legitimate user identifications (ID's) with respective passwords, fingerprint, pattern, or any other type of security information for recognition by the computer system. *Id.* at 3:55–60. If there is a match between the user inputs, within the designated time, and stored security information, the compare circuit 150 issues a "pass" signal to computer system 100. *Id.* at 65–67.

3. Anderson Ex. (1006)

We make the following finding of facts concerning Anderson.

Anderson also discloses a system and method for authenticating an authorized user to access a secured device. Anderson's disclosed system inputs an access code "via temporal variations in the amount of pressure applied to a touch interface." Ex. 1006, Abstr.

Anderson's method of inputting an access code uses digitizer pad 120 as a touch interface, which may include an optical scanner or thermal sensor for collecting an image of the user's fingerprint. Ex. 1006, 5:43–44, 7:4–7. The user enters the access code as a series of pressure pulses having varying durations. *Id.* at 6:45–47. This fingerprint access code is then compared with a stored code template to determine whether they match. If they do, access is permitted. *Id.* at 6:48–54.

Anderson discloses a system where the touch interface may sense only "temporal applications of pressure," relying on *timing* of the pressure applications for entry of the access code. Ex. 1006, 7:28–30; Fig. 4A. Alternately, as shown in FIG. 4B, the touch interface may sense both temporal applications of pressure and variations in pressure magnitude or intensity. *Id.* at 7:34–37. Thus, the access code would be entered as a series

of alternating short and long pressure applications that vary both in duration and magnitude. *Id.* at 7:37–39.

Annotated Figures 4A from Anderson is reproduced below.

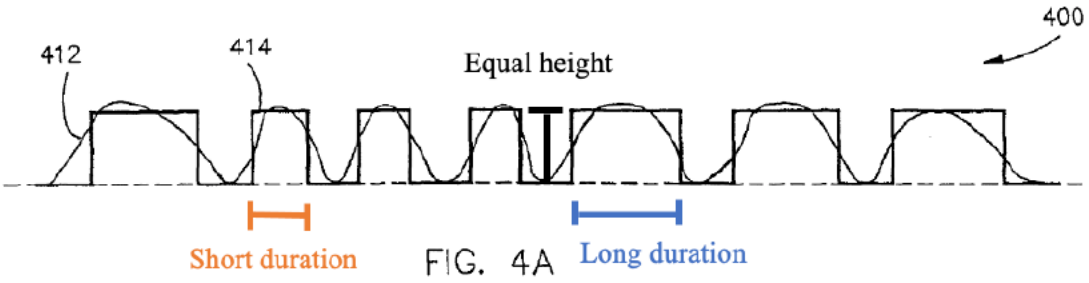


FIG. 4A

Figure 4A from Anderson is a diagram illustrating entry of an access code via temporal pressure variation. Ex. 1006, 2:65–67. The annotations are provided by Dr. Sears in his declaration testimony. Ex. 1003 ¶ 100. As explained by Dr. Sears, in Figure 4A, "the height of each bar the same because the magnitude or intensity of the finger pressure press is not detected. However, at least some of the presses have a different duration than other presses, as represented by the width of each bar." *Id.*

Annotated Figure 4B from Anderson is reproduced below.

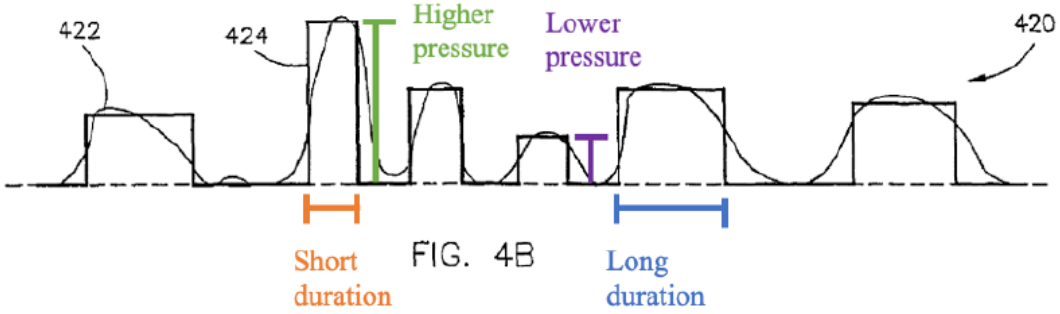


FIG. 4B

Figure 4B from Anderson is a diagram illustrating entry of an access code via temporal pressure variation. Ex. 1006, 2:65–67. The annotations are provided by Dr. Sears in his declaration testimony. Ex. 1003 ¶ 101. As explained by Dr. Sears, Figure 4B "illustrates variations in both the amount

of pressure applied using the height of each bar and the duration of the applied pressure using the width of each bar." *Id.*

a) Analysis of Independent Claim 1

Petitioner provides a clause-by-clause analysis of independent claim 1, identifying where in each of the cited references, Mathiassen, McKeeth, or Anderson, the claimed element is disclosed, and why it would have been obvious to a person of ordinary skill to combine the various disclosed elements with a reasonable expectation of success. *See* Pet. 50–56. Throughout its analysis, Petitioner cites the Declaration testimony (Ex. 1003) of Dr. Sears for evidentiary support.

For ease of reference and consistency, we will refer to Petitioner's Claim Listing Appendix convention, as did Patent Owner.

Patent Owner asserts that Petitioner has not met its burden to prove unpatentability because:

(1) Mathiassen, alone or in combination with other references, does not disclose the "accessibility attribute" limitation, as properly construed, and, moreover, there is no motivation to combine Mathiassen with the other references (PO Resp. 12–23);

(2) Anderson, alone or combined with Mathiassen, does not disclose the "biometric signal duration limitation," and, also, there is no motivation to combine Anderson and Mathiassen (*id.* at 24–30);

(3) the references, alone or in combination, do not "populate" the database according to an "instruction" (*id.* at 30–33); and

(4) there were simpler solutions available to a skilled person than the Mathiassen/Anderson combination (Sur-reply 4–8).

Patent Owner states these same arguments apply to independent claims 9 and 10, as well as to the challenged dependent claims. *Id.* at 33.

Patent Owner's defenses are based in large part on accepting Patent Owner's asserted claim constructions, which we have *not* done.

We begin our claim analysis with claim 1.

b) Preamble
"A system for providing secure access to a controlled item."

Petitioner asserts that "[t]o the extent the preamble is limiting, Mathiassen teaches a system for providing secure access to a controlled item." Pet. 50 (citing Mathiassen, Abstr., ¶¶ 145–147).

Patent Owner does not contest specifically Petitioner's arguments with respect to the preamble of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests the preamble of claim 1.

c) Limitation 1(a)
"a database of biometric signatures"

Petitioner asserts that Mathiassen discloses a stored database of tables. Pet. 14–16 (citing Ex. 1004, ¶¶ 50, 147, Fig. 2B; Ex. 1003 ¶¶ 117–121.

Patent Owner does not contest specifically Petitioner's arguments with respect to the limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(a).

d) Limitation 1(b)
"a transmitter sub-system"

Petitioner asserts Mathiassen teaches a transmitter subsystem, including transceiver 27, fingerprint sensor 5, processor 2 (of integrated circuit 1) executing administrative code, and non-volatile memory 7, 7A,

each housed in portable control 20. Pet. 16, 17 (citing Ex. 1004 ¶¶ 185–188; Ex. 1003 ¶¶ 122–125).

Patent Owner does not contest specifically Petitioner's arguments with respect to the limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(b).

e) Claim 1(b1)
"a biometric sensor for receiving a biometric signal"

Petitioner asserts that Mathiassen's "fingerprint sensor 5" is a "biometric sensor for receiving a biometric signal" because it detects a finger on the sensor and processes raw images of fingerprints. Pet. 18 (citing Ex. 1004 ¶ 49; Ex. 1003 ¶¶ 126–127).

Patent Owner does not contest specifically Petitioner's arguments with respect to the limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(b1).

f) Claim 1(b2)
"means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute"

Based on the claim constructions discussed in Section II.C. of this Decision, the disclosed structure for this means-plus-function clause is a "database and computer program product having a computer readable medium having a computer program recorded therein." Pet. 6.

Petitioner asserts "Mathiassen teaches fingerprint sensor 5 of portable control 20 receiving a fingerprint reduced to access minutiae and comparing

such access minutiae to master minutiae tables (i.e., database) to authenticate a user." Pet. 51 (citing Ex. 1004 ¶¶ 71–72, 175–180; Ex. 1003 ¶ 279).

Petitioner's application of the references is as follows:

> *Mathiassen* and *McKeeth* each teaches **whether** access is granted. In *Mathiassen*, access *is granted* (as opposed to denied) by opening (i.e., unlocking) the car doors. *Mathiassen*, [0181-0182]; *Dec.,* 241. The issued "open door" command indicates "whether" access should be granted. *Mathiassen* teaches the open door command is issued in response to access minutiae matching a stored biometric signature of the car owner/administrator. *Mathiassen,* [0182]; *Dec.,* 241. In contrast, if the processor 2 does not find a match, then no access will be granted because "the process will be aborted." *Mathiassen,* [0181]. Thus, the "open door" command indicates that access should be granted.

Pet. 41–42.

Here, consistent with the proposed construction, Petitioner relies solely on Mathiassen to satisfy the proposed claim construction of an attribute that establishes whether and *under which conditions* access to the controlled item should be granted to a user. If the processor 2 in Mathiassen does not find a match, then no access will be granted. *Id.* Petitioner also, separately, asserts that McKeeth discloses a system in which "access is granted where 'there is a match between the input and security information.'" *Id.* at 42 (citing Ex. 1005, 3:65–67, 3:11–28).

McKeeth discloses different types of input security information, including audio sensors to detect a voice recognition and an optical scanner for fingerprint and/or retina scans. Ex. 1005, 3:1–10. Any one or more, or all, of the described types of input signals may be used to authenticate a user. *Id.* at 3:11–12. If the input and security information do not match the

stored information, the compare circuit issues a "flag signal" indicating denial of access by the user." *Id.* at 4:2–4.

Petitioner concludes that Mathiassen and McKeeth "each teaches **under what conditions** access is granted." Pet. 42. "Specifically, both references teach outputting an accessibility attribute upon there being a match of a live or access biometric signal to a stored biometric signal." *Id.* Petitioner notes that McKeeth "teaches both a duress instruction and an alert instruction when there is no match," but the duress instruction is distinct from the conditions under which access is, or is not, granted. *Id.*

Patent Owner asserts that Mathiassen either grants or denies access but does not provide any other condition or alternative "beyond the 'whether' inquiry, and Apple's reading of Mathiassen consequently merges the 'whether' and 'under which conditions' components of its own construction of the 'accessibility attribute' limitation." PO Resp. 13. Further, Patent Owner asserts that the Board ignored the "under which conditions" aspect in adopting Petitioner's construction of the "accessibility attribute." *Id.* at 14.

Patent Owner reasons that "[u]nder the Board's treatment of Mathiassen, a binary decision limited to access/abort satisfies both the 'whether' and 'under which conditions' requirement for 'accessibility attribute.'" PO Resp. 15. Patent Owner misconstrues our analysis of Mathiassen, as we have explained above based on our construction of the term "accessibility attribute."

Our construction of the "accessibility attribute" allows for conditional access, if any conditions are imposed, or unconditional access, if no conditions are imposed. Patent Owner's arguments fail to account for this construction.

Patent Owner argues that there is no motivation to combine Mathiassen and McKeeth because there were simpler alternative solutions available, the existence of which undermines the motivation to combine. PO Resp. 19–23; Sur-reply 4–8. This argument is inconsistent with controlling caselaw that makes clear "[i]t's not necessary to show that a combination is the *best* option, only that it be a *suitable* option." *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1380 (Fed. Cir. 2023) (citing *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 784, 800 (Fed. Cir. 2021) (quoting *PAR Pharm., Inc. v. TWI Pharms., Inc.*, 773 F.3d 1186, 1197–98 (Fed. Cir. 2014) (emphasis in original)); *see also Netflix, Inc. v. DivX, LLC*, No. 2022-1083, 2023 WL 2298768, at *5 (Fed. Cir. Mar. 1, 2023) (citing *In re Mouttet*, 686 F.3d 1322, 1334 (Fed. Cir. 2012) and *In re Kahn*, 441 F.3d 977, 990 (Fed. Cir. 2006)).

The motivation-to-combine analysis is a flexible one. "*[A]ny* need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *KSR*, 550 U.S. at 420 (emphasis added). And "[a] person of ordinary skill is also a person of ordinary creativity, not an automaton." *Id.* at 421. Thus, "in many cases[,] a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle." *Id.* at 420. The motivation-to-combine analysis "need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court [or this Board] can take account of the inferences and creative steps that a person of ordinary skill in the art would employ." *Id.* at 418.

Here, based on our claim construction and analysis of the references, we determine that Petitioner establishes the claimed "accessibility attribute."

g) Claim 1(b3)
"means for emitting a secure access signal conveying information"

Based on the claim constructions discussed above, the disclosed structure for this means-plus-function clause is a "computer program product having a computer readable medium having a computer program recorded therein" for performing the claimed function. Pet. 7 (citing Ex. 1073).

Petitioner asserts Mathiassen discloses the "means for emitting," which is "administrative code," (e.g., algorithm) stored in non-volatile memory 7, 7A generating the encrypted "open door" command (i.e., secure access signal) and directing the transceiver to transmit the signal to the ignition control of the car. Pet. 52 (citing Ex. 1003 ¶¶ 281, 282).

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(b3).

h) Claim 1(c)
"a receiver sub-system"

Petitioner asserts Mathiassen discloses a receiver sub-system, which includes ignition control 15, central car computer, and "transceivers of the door locks and the central car computer." Pet. 25 (citing Ex. 1004 ¶¶ 186–187). Petitioner also asserts the central car computer includes a transceiver receiving the signal (e.g., "open door" command) from portable control 20. *Id.* (citing Ex. 1003 ¶¶ 169–171; Ex. 1004 ¶¶ 149, 167, 186). According to

Petitioner, a "transceiver," as disclosed in Mathiassen, "is well understood by a POSITA[20] to include a receiver." Pet. 25 (citing Ex. 1003 ¶ 173).

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(c).

i) Claim 1(c1)
"means for receiving the transmitted secure access signal"

Based on the claim constructions discussed above, the disclosed structure for this means-plus-function clause is receiver 118. Pet. 7 (citing Ex. 1079).

Petitioner asserts Mathiassen discloses a receiver sub-system comprising the ignition control 15, central car computer, and "transceivers of the door locks and the central car computer." Pet. 52, 25 (citing Ex. 1004 ¶¶ 186–187). The central car computer includes a transceiver receiving the signal (e.g., "open door" command) from portable control 20. *Id.* (citing Ex. 1003 ¶¶ 169–171; Ex. 1004 ¶¶ 149, 167, 186). According to Petitioner, both the door locks and central car computer in Mathiassen include a transceiver. *Id.* (citing Ex. 1004 ¶ 186; Ex. 1003 ¶¶ 170–172). Petitioner

[20] "POSITA" is a commonly used patent law acronym for a "person of ordinary skill in the art." *See* 35 U.S.C. § 103(a) stating a statutory standard for obtaining a patent ("A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 , if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made *to a person having ordinary skill in the art* to which said subject matter pertains.") (emphasis added).

also asserts that "[a] 'transceiver' is well understood by a POSITA to include a receiver." Pet. 52, 25 (citing Ex. 1003 ¶ 13).

Petitioner also asserts that the signal received by the car computer's transceiver is sent either to the ignition control processor or the car computer's processor for decryption. Pet. 52, 25–26 (citing Ex. 1004 ¶¶ 187–188). After decrypting the command, a "similar encrypted command will be relayed to the door locks by the car computer," i.e., part of the mapped "receiver sub-system." *Id.* at 26; Ex. 1003 ¶ 170.

Petitioner concludes that Mathiassen's disclosed transceiver "performs the function of 'receiving the secure access signal,' (e.g., 'open door' command) transmitted from the transceiver 27 of portable control 20, Pet. 52, 26 (citing Ex. 1003 ¶¶ 170–171, 174; Ex. 1004 ¶ 186).

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(c1).

j) Claim 1(c2)
"means for providing conditional access to the controlled item dependent upon said information"

Based on the claim constructions discussed above, the disclosed structure for this means-plus-function clause is "controller 109 executing software 304." Pet. 7–8 (citing Ex. 1079).

Similar to the analysis for clause 1(c1) discussed above, Petitioner asserts "Mathiassen's processor of the ignition control, central car computer, or both, individually or collectively, comprise the "controller" structure. Pet. 26 (citing Ex. 1003 ¶¶ 176–183). As explained by Petitioner,

Mathiassen teaches two implementations: "a first in which the ignition control decrypts and authenticates the received command," and "a second in which the central car computer decrypts and authenticates the command." Pet. 27 (citing Ex. 1003 ¶¶ 177–183). Dr. Sears' testimony explains that a person of ordinary skill "would have understood that for the central car 'computer' to perform such algorithms, it includes or otherwise renders obvious a processor, as these same algorithms are disclosed as being performed by a processor when implemented in the ignition n control." Ex. 1003 ¶ 183. Dr. Sears also testifies that Mathiassen's "processor 2 of IC 1 in ignition control 15 performing decryption and authentication." *Id.*

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(c2).

k) Claim 1(d)
"wherein the transmitter sub-system further comprises means for populating the data base of biometric signatures"

Based on the claim constructions discussed above, the disclosed structure for this means-plus-function clause is "database and computer program product having a computer readable medium having a computer program recorded therein." Pet. 8–9 (citing Ex. 1077).

Petitioner asserts Mathiassen discloses administrative software that will "require a minimum of say 3 minutiae fingerprint representations of acceptable quality" that are stored in nonvolatile memory. Pet. 53 (citing Ex. 1004 ¶ 130). It is Petitioner's position that, in Mathiassen, the "administrative code directs the processor to store the acceptable fingerprint

representations in the form of master minutiae tables." Pet. 53 (citing Ex. 1004 ¶¶ 130–131; Ex. 1003 ¶ 287). According to Petitioner, "[s]toring master minutiae tables from a car owner or 'other users' is at least equivalent to the '208 Patent describing storing biometric signatures of an administrator and 'ordinary' users in database 105." *Id.* (citing Ex. 1004 ¶¶ 164–165, 190).

Petitioner also asserts that Mathiassen and McKeeth "enroll[ ] signatures indicating a user is under duress, which is at least equivalent to the '208 Patent describing storing a 'duress signature.'" Pet. 53. Petitioner concludes that "a POSITA would have understood or found it obvious that Mathiassen's administrative code in the non-volatile memory 7, 7A of IC 1 comprises the "means for populating." *Id.* (citing Ex. 1003 ¶ 287).

Patent Owner does not contest specifically Petitioner's arguments with respect to the limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(d).

l) *Claim 1(d1)*
"means for receiving a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry"

Based on the claim constructions discussed above, the disclosed structure for this means-plus-function clause is "computer program product having a computer readable medium having a computer program recorded therein." Pet. 8 (citing Ex. 1079).

Petitioner asserts that "Mathiassen's sensor receives a series of entries of the biometric signal by a movement analyzing program identifying the fingerprint motions." Pet. 54. According to Petitioner, the representations

"are generated once a finger is detected on the sensor surface, which is at least equivalent to the '208 Patent checking a biometric is received on the biometric sensor." *Id.* (citing Ex. 1004 ¶ 49).

Petitioner also asserts that "Anderson [Ex. 1006] teaches receiving a series of fingerprint pressure pulses of varying duration." Pet. 54 (citing Ex. 1006, 7:28–34, Fig. 4A). As we explained above in our discussion of Anderson, there can be no reasonable dispute that Anderson discloses input biometric signals that vary in number and duration.

As explained by Petitioner,

> In *Mathiassen*, the series of directional finger movements instruct a command on *Mathiassen's* portable device (as modified by *McKeeth*). A POSITA would have been motivated and found it obvious to substitute or modify such directional finger movements with a series of presses of varying duration, as taught by *Anderson*, for instructing a command at portable device 20.

Id. at 35 (citations omitted).

Petitioner also provides argument and probative evidence as to why a person of ordinary skill would have combined the disclosures of the references, with a reasonable expectation that the combination would be successful. Pet. 35–36. As explained by Petitioner,

> There would have been a reasonable expectation of success in modifying *Mathiassen's* control 20, because it contains software and hardware for detecting directional movement and touch/no touch. *Mathiassen's* sensor 5 already detects a finger press because it receives fingerprint representations. The modification therefore only requires simple programming techniques (e.g., modifying the translation program to count the number and duration of "touch" or "no touch") that were within a POSITA's expertise.

Id. at 36.

Patent Owner asserts that the "pressure pulses" in Anderson do not generate biometric signals because they are captured "as the pressure code is entered," and are therefore not part of the pressure code itself. *See* PO Resp. 25. Patent Owner also explains that "combining Mathiassen's fingerprint sensor with Anderson's pressure code does not produce the claimed invention, as any duration would apply to a nonbiometric signal." *Id.* (citing Ex. 2011 ¶¶ 69-71). Dr. Easttom testifies that Anderson does not capture a biometric signal. Ex. 2011 ¶¶ 69–71. Petitioner, however, relies on Mathiassen and McKeeth for the biometric sensing, but relies on Anderson, which suggests the benefits and options of using a number and duration of pulses as inputs. *E.g.*, Pet.32–36 Because Mathiassen, like the '208 patent, uses a biometric sensor as the input device, it will detect the biometric part of the input signal, while also sensing the number and duration of inputs.

Patent Owner also asserts that a "simpler combination" was available. PO Resp. 28. According to Patent Owner, "a simpler solution would have been to add Anderson's pushbutton to Mathiassen's key fob." *Id.* at 29 (citing Ex. 2011 ¶ 80). As explained above, "[i]t's not necessary to show that a combination is the *best* option, only that it be a *suitable* option." *Intel Corp.*, 61 F.4th at 1380 (citations omitted).

Based on the Petitioner's arguments and evidence summarized above, we determine Petitioner has sufficiently shown that the cited references, as combined by Petitioner, disclose or suggest limitation 1(d1).

m) Claim 1(d2)
"means for mapping said series[of entries of the biometric signal] into an instruction"

Based on the claim constructions discussed above, the disclosed structure for this means-plus-function clause is "computer program product

having a computer readable medium having a computer program recorded therein." Pet. 8 (citing Ex. 1077).

Petitioner asserts Mathiassen discloses the "software translation program" executed by the processor in integrated circuit 1 performs the function of "mapping said series into an instruction" by translating the series of finger movements to a command in a command table. Pet. 55 (citing Ex. 1004 ¶ 192). The cited disclosure in Mathiassen states:

> As an additional safety feature the portable or embedded device could be equipped with means for the input of code or commands. This is achieved by defining a fingerprint storage segment in non-volatile memory (7, 7A or 7E) where the device may store a series of consecutive fingerprint representations generated by the fingerprint sensor signal capturing and pre-processing block (5C). *Movement analyzing means, in the form of a hardware or a software movement analyzing program module analyzes the obtained series of fingerprint representations to obtain a measure of the omni-directional finger movements across the sensor in two dimensions. Translation means in the form of a hardware or a software translation program module analyzes and categorizes the omni-directional finger movements across the fingerprint sensor according to predefined sets of finger movement sequences* including directional and touch/no-touch finger movement sequences. *A command table is used to translate the categorized finger movements into control signals whereby the translating means generates control signal for controlling the device, e.g. the stand-alone appliance, in response to the finger movements on the sensor.*

Ex. 1004 ¶ 192 (emphases added). Based on this cited disclosure from Mathiassen, there can be no reasonable dispute that Mathiassen discloses a computer implemented software translation program for converting finger movements into control signals. *See also* Pet. 54 (explaining that

Mathiassen's sensor receives a series of entries of the biometric signal by a movement analyzing program identifying the fingerprint motions).

n) Claim 1(d3)
"means for populating the data base according to the instruction"

Based on the claim constructions discussed above, the disclosed structure for this means-plus-function clause is "database and computer program product having a computer readable medium having a computer program recorded therein" with code for performing the claimed function Pet. 8–9 (citing Ex. 1077).

Petitioner asserts "Mathiassen-McKeeth teaches or renders obvious administrative code directing processor 2 of portable door control to store fingerprint representations (from sensor 5) in master minutiae tables (i.e., database of biometric signatures) stored in memory 7, 7A when enrolling a new user, a car owner (i.e., administrator), or a duress signature." Pet. 55–56. Petitioner also argues that "Mathiassen discloses, for the medicine cabinet embodiment, the administrator initiates enrollment of 'the next user' by 'authenticating himself by his fingerprint.'" *Id.* at 37 (citing Ex. 1004 ¶ 131). According to Petitioner, enrolling new users includes "creating master minutiae tables subsequently stored in memory 7, 7A, i.e., the 'populating the database.'" *Id.* (citing Ex. 1004 ¶ 71; Ex. 1003 ¶¶ 222–224).

Patent Owner argues that "*Mathiassen* has no teaching that either the 'predefined sets of finger movement sequences' or the 'command table' constitute a series of received biometric signal entries that are mapped into an instruction used to populate the database as part of the enrollment process." PO Resp. 31.

Petitioner asserts that "Mathiassen teaches receiving entries of a series of fingerprints" and that "Anderson teaches receiving a series of fingerprint

pressure pulses of varying duration." Pet. 54 (citing Ex, 1004 ¶ 192 and Ex. 1006, 7:28–34). As Petitioner correctly states, "Mathiassen's fingerprint sensor receives this series of entries of the biometric signal, similar to the '208 Patent's code entry module 103 containing a biometric sensor 121 that receives a user's fingerprint." Pet. 55. Mathiassen's processor translates the series of fingerprints (received by its biometric sensor into a command, such as "open door" command, for authenticating the user to access the car doors. Ex. 1004 ¶ 192.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that the cited disclose or suggest limitation 1(d3).

o) Claim 1(e)
"wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device"

Petitioner asserts "Mathiassen teaches the controlled item is a 'locking mechanism of a physical access structure' (i.e., the car door locks of the central locking system)." Pet. 49 (citing Ex. 1004 ¶ 187; Ex. 1003 ¶ 266 (testifying that "Mathiassen teaches a controlled item that is 'a locking mechanism of a physical access structure,'" [*i.e.* a car door])). We also note that Mathiassen clearly discloses use of its disclosed computer-based locking and access system on a "laptop computer," "hotel safe," "medicine cabinet," and as a "door control" in "automotive applications." Ex. 1004 ¶¶ 41–44, 109–113.

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(e).

4. Conclusion for Independent Claim 1

Based on the evidence and our analysis above, we determine that Petitioner has established by a preponderance of the evidence that claim 1 of the '208 patent would have been obvious, and thus is not patentable.

5. Independent Claims 9 and 10

Patent Owner concedes that patentability of independent claims 9 and 10 stands or falls with patentability of independent claim 1. PO Resp. 33. Thus, applying the same analysis and evidence as discussed above in the context of claim 1, we determine that Petitioner has established by a preponderance of the evidence that independent claims 9 and 10 of the '208 patent would have been obvious, and thus are not patentable.

6. Dependent Claims 3–7, 9–11, 13

Petitioner provides an element-by-element analysis of where each element in the challenged claims 3–7, 9–11, and 13 is disclosed in, or would have been obvious in view of, the cited references. Pet. 12–63. For clauses in claims 3–7, 9–11, and 13 that are similar to those in claim 1, Petitioner refers to its arguments for claim 1, or other claims. *See, e.g.*, Pet. 62–63 (referring to its analysis for claims 1 and 10). Petitioner also provides a reason why it would have been obvious to modify and combine the references with a reasonable expectation of success, as proposed by Petitioner. *Id.* Petitioner relies throughout the analysis of these claims on the testimony of Dr. Sears (Ex. 1003) for evidentiary support.

Patent Owner concedes that patentability of dependent claims 3–7, 9–11, and 13 depend on its arguments for patentability of independent claim 1.

PO Resp. 33. Thus, applying the same analysis and evidence as discussed above in the context of claim 1, we determine that Petitioner has established by a preponderance of the evidence that dependent claims 3–7, 9–11, and 13 of the '208 patent would have been obvious, and thus are not patentable.

III. CONCLUSION[21]

Petitioner has established by a preponderance of the evidence that claims 1, 3–7, 9–11, and 13 are unpatentable.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, that Petitioner has shown by a preponderance of the evidence that claims 1, 3–7, 9–11, and 13 are unpatentable.

[21] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

V. SUMMARY TABLE

Claim(s)	35 U.S.C. §	Reference(s)/Basis	Claim(s) Shown Unpatentable	Claim(s) Not shown Unpatentable
1, 3–7, 9–11, 13	103	Mathiassen, McKeeth, Anderson	1, 3–7, 9–11, 13	
Overall Outcome			1, 3–7, 9–11, 13	

IPR2022-00601
Patent 9,269,208 B2

For PETITIONER:

Jennifer C. Bailey
Adam P. Seitz
ERISE IP, P.A.
jennifer.bailey@eriseip.com
adam.seitz@eriseip.com

For PATENT OWNER:

Darlene Ghavimi-Alagha
Brian Bozzo
K&L GATES LLP
darlene.ghavimi@klgates.com
brian.bozzo@klgates.com

Trials@uspto.gov
571-272-7822

Paper 31
Date: September 27, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

CPC PATENT TECHNOLOGIES PTY, LTD.,
Patent Owner.

IPR2022-00602
Patent 9,665,705 B2

Before SCOTT A. DANIELS, BARRY L. GROSSMAN, and AMBER L. HAGY, *Administrative Patent Judges.*

GROSSMAN, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

A. Background and Summary

Apple Inc. ("Petitioner" or "Apple") filed a Petition for *inter partes* review of claims 1, 4, 6, 10–12, and 14–17 (collectively, the "challenged claims") of U.S. Patent No. 9,655,705 B2 (Ex. 1001, "the '705 patent"). Paper 1 ("Pet."). CPC Patent Technologies PTY, Ltd. ("Patent Owner" or "CPC") timely filed a Preliminary Response to the Petition. Paper 7 ("Prelim. Resp."). With our authorization, Petitioner filed a Preliminary Reply (Paper 8 ("Prelim. Reply")) addressing the issue of discretionary denial raised in the Preliminary Response and Patent Owner filed a Prelim. Sur-Reply (Paper 9 ("Prelim. Sur-Reply")).

We concluded that Petitioner satisfied the burden, under 35 U.S.C. § 314(a), to show that there was a reasonable likelihood that Petitioner would prevail with respect to at least one of the challenged claims. Accordingly, on behalf of the Director (37 C.F.R. § 42.4(a)), and in accordance with *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1353 (2018), we instituted an *inter partes* review of all the challenged claims, on all the asserted grounds. Paper 11 ("Dec. Inst.").

Patent Owner filed a Response. Paper 17 ("PO Resp."). Petitioner filed a Reply. Paper 20 ("Reply"). Patent Owner filed a Sur-reply. Paper 26 ("Sur-reply").

Petitioner submitted eighty exhibits. *See* Exs. 1001–1091[1] (some consecutive exhibit numbers were *not* used; *e.g*, there are no exhibits

[1] Exhibit 1091 is a demonstrative exhibit used at the final hearing. It is not an evidentiary exhibit. See PTAB Consolidated Trial Practice Guide, 84 (Nov. 2019 ("TPG") ("Demonstrative exhibits used at the final hearing are aids to oral argument and not evidence").

numbered 1056–1064); *see also* Paper 28 (Petitioner's Updated Exhibit List stating that Exhibit numbers 1056–1064 were "Intentionally left blank."). Petitioner relies on the Declaration testimony of Andrew Sears, Ph.D. *See* Exs. 1003, 1090.

Patent Owner submitted sixteen exhibits. *See* Exs. 2001–2016[2]; *see also* Paper 29 (Patent Owner's Updated Exhibit List). Patent Owner relies on the Declaration testimony of William C. Easttom III, D. Sc,, Ph.D. *See* Exs. 2013, 2014.

A hearing was held June 29, 2023. (Paper 30) ("Transcript or "Tr.").

We have jurisdiction under 35 U.S.C. § 6. We enter this Final Written Decision pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

Petitioner has the burden of proving unpatentability of a claim by a preponderance of the evidence. 35 U.S.C. § 316(e).

Based on the findings and conclusions below, we determine that Petitioner has proven that claims 1, 4, 6, 10–12, and 14–17 are unpatentable.

B. Real Parties-in-Interest

Apple identifies itself as the sole real party-in-interest. Pet. 62.

CPC also identifies itself as the sole real party-in-interest. Paper 4, 2.

C. Related Matters

Petitioner and Patent Owner each identify the following two district court proceedings as related matters: (1) *CPC Patent Technologies Pty Ltd. v. Apple Inc.,* Case No. 6:21-cv-00165-ADA (W.D. Tex.); and (2) *CPC Patent Technologies Pty Ltd. v. HMD Global Oy,* Case No. 6:21-cv-00166-ADA (W.D. Tex.) (the "HMD W.D. Texas case"). Pet. 62; Paper 4, 2.

[2] Exhibit 2016 is a demonstrative exhibit used at the final hearing. It is not an evidentiary exhibit. *See id.*

The first listed case, between the same parties involved in this *inter partes* review proceeding, however, has been transferred to the Northern District of California. *See In re Apple Inc.*, 2022 WL 1196768 (Fed. Cir. Apr. 22, 2022); *see also* Ex. 3002 (Text Order granting Motion to Change Venue). The case is now styled *CPC Patent Technologies Pty Ltd. v. Apple Inc.*, No. 5:22-cv-02553 (N.D. Cal.) (the "Apple N.D. California case"). *See* Ex. 3003 (PACER Docket for the transferred case); Prelim. Resp. 1, fn 1 (Patent Owner acknowledging the transfer from the Western District of Texas to the Northern District of California).

Petitioner and Patent Owner also each identify the following two pending *inter partes* review proceedings as related matters: (1) IPR2022-00600, challenging claims in Patent 8,620,039; and (2) IPR2022-00601, challenging claims in Patent 9,269,208, which is the "parent" of the '705 patent. *See* Ex. 1001, code (63). A final written decision in the 00600 IPR is due October 17, 2023. A final written decision in the 00601 IPR is being issued simultaneously with this Decision in the case before us.

D. The '705 Patent

We make the following findings concerning the disclosure of the '705 patent.

The '705 patent discloses a system "for providing secure access to a controlled item." Ex. 1001, Abstr. The "controlled item" can be, for example, the locking mechanism of a door or an electronic lock on a personal computer. *Id.* at 1:43–46.[3] The system uses a database of "biometric signatures" (*id.* at2:32), such as a fingerprint (*id.* at 7:36) for determining authorized access.

[3] Citations are to column:line[s] of the '705 patent.

Figure 2 from the '705 patent is reproduced below.

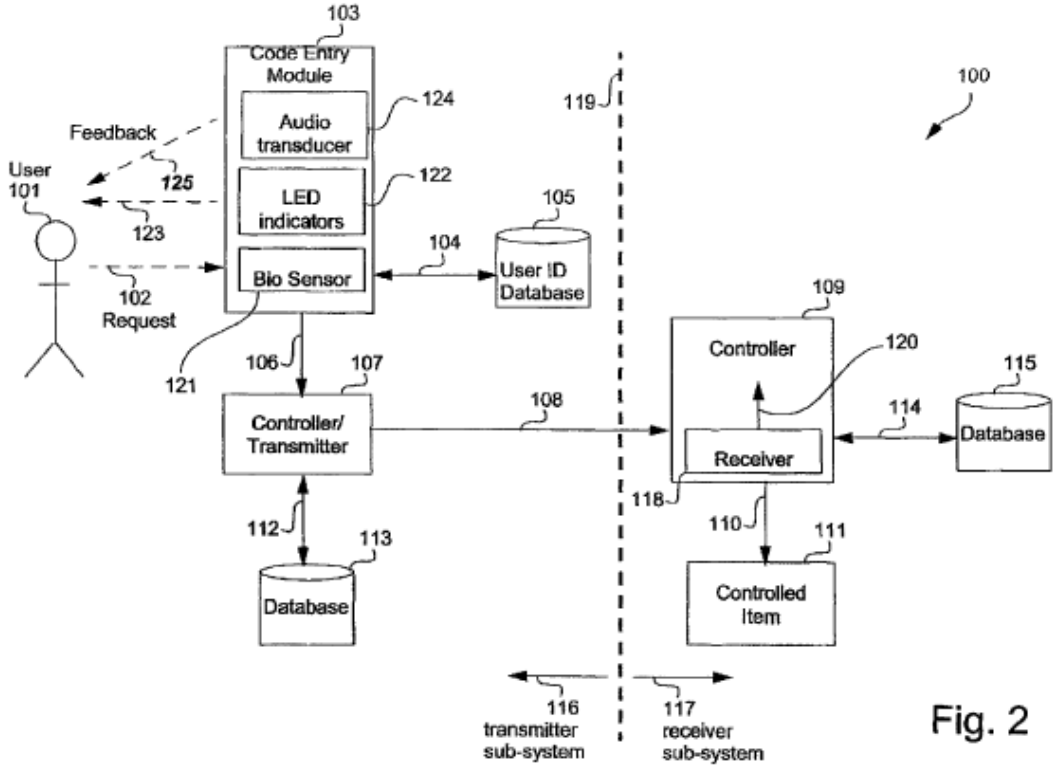


Fig. 2

Figure 2 is a functional block diagram of an arrangement for providing secure access according to the system disclosed in the '705 patent. Ex. 1001, 5:18–19.

As described in the written description of the '705 patent, and as illustrated generally in Figure 2, user 101 makes a request to code entry module 103. *Id.* at 5:56–57. Code entry module 103 includes biometric sensor 121. *Id.* at 5:57–58. If biometric sensor 121 is a fingerprint sensor, for example, then the request "typically takes the form of a thumb press" on a sensor panel (not shown) on code entry module 103. *Id.* at 5:60–63. "Other physical attributes that can be used to provide biometric signals include voice, retinal or iris pattern, face pattern, [and] palm configuration." *Id.* at 1:30–32; *see also id.* at 16:45–49 (claim 4 stating "the biometric sensor

is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration").

Code entry module 103 then "interrogates" an authorized user identity database 105, which contains "biometric signatures" for authorized users, to determine if user 101 is an authorized user. Ex. 1001, 5:64–6:2. If user 101 is an authorized user, code entry module 103 sends a signal to "controller/transmitter" 107. *Id.* at 6:2–4. Database 105 is prepared by an "administrator." *Id.* at 10:38–42 ("The first user of the code entry module 103 . . . is automatically categorised[4] as an administrator.").

The disclosed system and method compare biometric input "*signal*" 102 to database 105 of authorized biometric "*signatures*" to determine if user 101 is an authorized user. *Id.* at 5:65–6:2 ("Thus for example if the request 102 is the thumb press on the biometric sensor panel 121 [producing a thumbprint] then the user database 105 contains biometric signatures [*i.e.,* thumbprints] for authorised users against which the request 102 can be authenticated."). If user 101 is an authorized user, code entry module 103 sends a signal to "controller/transmitter" 107 allowing access to the controlled item. *Id.* at 6:2–10.

When biometric sensor 121 is a fingerprint sensor,[5] the biometric signatures stored in database 105 are not limited to a single fingerprint. The '705 patent also discloses that, if so programed by an administrator, code

[4] The Specification uses the British spelling, which we also use when quoting the Specification.
[5] *See* Ex. 1001, 10:35 – 38 ("Although the present description refers to 'Users', in fact it is 'fingers' which are the operative entities in system operation *when the biometric sensor 121 (see FIG. 2) is a fingerprint sensor*.") (emphasis added). Thus, it is clear that biometric sensor 121 is *not* limited to a fingerprint sensor.

entry module 103 may be activated by providing a succession of finger presses to biometric sensor 121 included in module 103. *Id.* at 10:56–58. If these successive presses are of the appropriate duration, the appropriate quantity, and are input within a predetermined time, controller 107 accepts the presses "as potential control information," or a biometric signal, and checks the input information against a stored set of "legal [authorized] control signals," or the database of biometric signatures. *Id.* at 10:59–67. "In one arrangement, the control information is encoded by *either or both* (a) the number of finger presses and (b) the relative duration of the finger presses." *Id.* at 10:60–63 (emphasis added).

An example of this type of "control information" or "legal control signal" is "dit, dit, dit, dah," where "dit" is a finger press of one second's duration . . . and "dah" is a finger press of two second's duration."[6] *Id.* at 11:1–7.

[6] We have not been directed to any persuasive evidence, and have found none on our own review of the evidence, which establishes why the Specification refers to the number and duration of finger presses as "control information" and "legal control signals," rather than a "biometric signal" and a "database" of "biometric signatures," respectively, which are the terms used throughout the Specification for the input signal and the database of authorized users.
The Specification is required to include "a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art . . . to make and use the same." 35 U.S.C. § 112(a). Neither we nor the parties, however, have jurisdiction in this *inter partes* review proceeding to address this enablement issue. *See id.* at § 311(b) ("A petitioner in an inter partes review may request to cancel as unpatentable 1 or more claims of a patent only on a ground that could be raised under section 102 or 103 and only on the basis of prior art consisting of patents or printed publications.").

If user 101 is an authorized user based on the inputs to code entry module 103, controller/transmitter 107 then sends "an access signal," based on a "rolling code," to controller 109. Ex. 1001, 6:2–9. According to the written description, "[t]he rolling code protocol offers non-replay encrypted communication." *Id.* at 6:9–10. Other secure codes, such as "the Bluetooth™ protocol, or the Wi Fi™ protocols" also can be used. *Id.* at 6:32–38.

If controller 109 determines that the rolling code received is "legitimate," then controller 109 sends a command to "controlled item 111," which, for example "can be a door locking mechanism on a secure door, or an electronic key +circuit in a personal computer" that is to be accessed by user 101. *Id.* at 6:11–20.

Code entry module 103 also incorporates at least one mechanism for providing feedback to user 101. *Id.* at 6:24–25. This mechanism can, for example, take the form of "one or more Light Emitting Diodes (LEDs) 122," and/or audio transducer 124, which provide visual or audio feedback to the user. *Id.* at 6:25–31.

In Figure 2, "sub-system 116," shown on the left of vertical dashed line 119, communicates with "sub-system 117," shown on the right of dashed line 119, "via the wireless communication channel" used by access signal 108 between controller/transmitter 107 and controller/receiver 109. *Id.* at 6:61–67. As disclosed in the '705 patent, "[a]lthough typically the communication channel uses a wireless transmission medium, there are instances where the channel used by the access signal 108 can use a wired medium." *Id.* at 7:9–14.

E. Illustrative Claim

Among the challenged claims, claims 1, 10, 11, 14, 15, 16, and 17 are independent claims.

Independent claims 1 and 15 are directed to a "system for providing secure access to a controlled item." Ex. 1001, 15:62–63; 18:39–40. These claims are identical except for claim 1 using the phrase "configured to," whereas claim 15 uses the phrase "capable of." For example, claim 1 includes "a biometric sensor *configured to receive* a biometric signal" (*id.* at 15:66–67 (emphasis added)), whereas claim 15 includes "a biometric sensor *capable of receiving* a biometric signal." (*id.* at 18:43–44 (emphasis added)). This same distinction also applies to the claimed elements of "a transmitter sub-system controller," "a transmitter," and "a receiver sub-system controller." *Compare id.* at 16:1–23 (claim 1) *with id.* at 18:45–67 (claim 15).

We discuss below in Section II.C (Claim Construction) whether use of the phrase "capable of" rather than the phrase "configured to" is a distinction without a substantive difference.

Independent claims 10 and 16 are directed to a "transmitter sub-system for operating in a system for providing secure access to a controlled item." *Id.* at 17:19–20; 19:1–2. The only distinction between claims 10 and 16 is the same "capable of"/"configured to" distinction discussed above for claims 1 and 15. *Compare id.* at 17:19–39 (claim 10) *with id.* at 19:1–20 (claim 16).

Independent claims 11 and 17 are directed to a "method for providing secure access to a controlled item." *Id.* at 17:40–41. The only distinction between claims 11 and 17 is the same "capable of"/"configured to" distinction discussed above for claims 1 and 15. Again, the only distinction

between claims 11 and 17 is the same "capable of"/"configured to" distinction discussed above for claims 1 and 15. *Compare id.* at 17:40–67 (claim 11) *with id.* at 19:21–20:23 (claim 17).

Independent claim 14 is directed to a "non-transitory computer readable storage medium storing a computer program." *Id.* at 18:18–19.

Independent claim 1 is illustrative and is reproduced below.

> 1. A system for providing secure access to a controlled item, the system comprising:
>
> a memory comprising a database of biometric signatures;
>
> a transmitter sub-system comprising:
>
> a biometric sensor configured to receive a biometric signal;
>
> a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and
>
> a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute; and
>
> a receiver sub-system comprising:
>
> a receiver sub-system controller configured to:
>
> receive the transmitted secure access signal; and
>
> provide conditional access to the controlled item dependent upon said information;
>
> wherein the transmitter sub-system controller is further configured to:
>
> receive a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;
>
> map said series into an instruction; and
>
> populate the data base according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

Ex. 1001, 15:62–16:23.[7]

F. Prior Art and Asserted Grounds

Petitioner asserts that the challenged claims are unpatentable on the following ground:

Claim(s) Challenged	35 U.S.C. §[8]	Reference(s)/Basis
1, 4, 6, 10–12, 14–17	103(a)	Mathiassen,[9] McKeeth,[10] Anderson[11]

Petitioner also relies on the declaration testimony of Andrew Sears, Ph.D. *See* Ex. 1003.[12]

[7] Petitioner provides a Claim Listing Appendix as part of the Petition. Pet. 64–69. This Appendix includes all the challenged claims identified by individual clause, such as, for claim 1, labeling the clauses 1(a), 1(b), 1(b)(1), etc. Petitioner refers to these clause labels in its analysis.
[8] The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284, 296–07 (2011), took effect on September 16, 2011. The changes to 35 U.S.C. §§ 102 and 103 in the AIA do not apply to any patent application filed before March 16, 2013. Because the application for the patent at issue in this proceeding has an effective filing date before March 16, 2013, we refer to the pre-AIA version of the statute.
[9] Mathiassen et al, US 2004/0123113 A1, published June 24, 2004 (Ex. 1004, "Mathiassen").
[10] McKeeth, US 6,766,456 B1, issued July 20, 2004 (Ex. 1005, "McKeeth").
[11] Anderson, US 6,509,847 B1, issued Jan. 21, 2003 (Ex. 1006, "Anderson").
[12] Exhibit 1003 is a 238-page declaration from Dr. Sears, including its Appendix A, which is a detailed mapping of the disclosures of the three applied references to the challenged claims. Dr. Sears currently is a Professor and Dean of the College of Information Sciences and Technology at The Pennsylvania State University. Ex. 1003 ¶ 5. Dr. Sears earned a Bachelor of Science degree in Computer Science, and a Ph.D. degree, also in Computer Science. *Id.* ¶ 6. He has held various positions in academia, including serving as the Interim Chief Information Security Officer at Penn State. *Id.* ¶¶ 7, 8. He has authored or edited a number of computer-related publications and held leadership positions in several computer industry organizations. *Id.* ¶¶ 10–12.

II. ANALYSIS

A. Obviousness

Section 103 forbids issuance of a patent when "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when available, evidence such as commercial success, long felt but unsolved needs, and failure of others.[13] *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966); *see KSR*, 550 U.S. at 407 ("While the sequence of these questions might be reordered in any particular case, the [*Graham*] factors continue to define the inquiry that controls."). The Court in *Graham* explained that these factual inquiries promote "uniformity and definiteness," for "[w]hat is obvious is not a question upon which there is likely to be uniformity of thought in every given factual context." *Graham*, 383 U.S. at 18.

The Supreme Court made clear that we apply "an expansive and flexible approach" to the question of obviousness. *KSR*, 550 U.S. at 415. Whether a patent claiming the combination of prior art elements would have been obvious is determined by whether the improvement is more than the predictable use of prior art elements according to their established functions.

[13] Patent Owner does not direct us to any objective evidence of non-obviousness in its Preliminary Response.

Id. at 417. To support this conclusion, however, it is not enough to show merely that the prior art includes separate references covering each separate limitation in a challenged claim. *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011). Rather, obviousness additionally requires that a person of ordinary skill at the time of the invention "would have selected and combined those prior art elements in the normal course of research and development to yield the claimed invention." *Id.*

In determining whether there would have been a motivation to combine prior art references to arrive at the claimed invention, it is insufficient to simply conclude the combination would have been obvious without identifying any reason *why* a person of skill in the art would have made the combination. *Metalcraft of Mayville, Inc. v. Toro Co.*, 848 F.3d 1358, 1366 (Fed. Cir. 2017).

Moreover, in determining the differences between the prior art and the claims, the question under 35 U.S.C. § 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. *Litton Indus. Prods., Inc. v. Solid State Sys. Corp.*, 755 F.2d 158, 164 (Fed. Cir. 1985) ("It is elementary that the claimed invention must be considered as a whole in deciding the question of obviousness."); *see also Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1537 (Fed. Cir. 1983) ("[T]he question under 35 U.S.C. § 103 is not whether the differences *themselves* would have been obvious. Consideration of differences, like each of the findings set forth in *Graham*, is but an aid in reaching the ultimate determination of whether the claimed invention *as a whole* would have been obvious.").

As a factfinder, we also must be aware "of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning." *KSR*, 550 U.S. at 421.

Applying these general principles, we consider the evidence and arguments of the parties.

B. Level of Ordinary Skill in the Art

The level of skill in the art is "a prism or lens" through which we view the prior art and the claimed invention. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). "This reference point prevents . . . factfinders from using their own insight or, worse yet, hindsight, to gauge obviousness." *Id.*

Factors pertinent to a determination of the level of ordinary skill in the art include: (1) educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology; and (6) educational level of workers active in the field. *Env't Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696–697 (Fed. Cir. 1983) (citing *Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.*, 707 F.2d 1376, 1381–82 (Fed. Cir. 1983)). Not all such factors may be present in every case, and one or more of these or other factors may predominate in a particular case. *Id.* Moreover, these factors are not exhaustive but are merely a guide to determining the level of ordinary skill in the art. *Daiichi Sankyo Co. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007). In determining a level of ordinary skill, we also may look to the prior art, which may reflect an appropriate skill level. *Okajima*, 261 F.3d at 1355.

"The *Graham* analysis includes a factual determination of the level of ordinary skill in the art. Without that information, a district court cannot

properly assess obviousness because the critical question is whether a claimed invention would have been obvious at the time it was made to one with ordinary skill in the art." *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986); *see also Ruiz v. A.B. Chance*, 234 F.3d 654, 666 (Fed. Cir. 2000) ("The determination of the level of skill in the art is an integral part of the *Graham* analysis.").

Neither party provides any persuasive evidence or argument concerning the factors identified above or any other factors relevant to determining the level of ordinary skill.

Petitioner asserts that a person of ordinary skill in the art would have had "at least a bachelor's degree in computer engineering, computer science, electrical engineering, or a related field, with at least one year experience in the field of human-machine interfaces and device access security." Pet. 4 (citing Ex. 1003 ¶¶ 31–35).[14] Petitioner also states that "[a]dditional education or experience may substitute for the above requirements." *Id.*

In forming an opinion on the level of ordinary skill applicable to this proceeding, Dr. Sears testifies that he considered various factors, including the type of problems encountered in the art, the solutions to those problems, the rapidity with which innovations are made in the field, the sophistication of the technology, and the education level of active workers in the field. Ex. 1003 ¶ 31. Dr. Sears also testifies that he "placed myself back in the time frame of the claimed invention and considered the colleagues with whom I had worked at that time." *Id.* Dr. Sears opines that a person of ordinary skill

[14] Petitioner cites this testimony as "Dec." Pet. 4, fn 1. We will cite it, as we do all other evidence, by reference to its Exhibit number, which is Exhibit 1003.

would have had the education and experience adopted by Petitioner. *Id.* at ¶ 32.

Patent Owner states it "does not dispute [Petitioner's] characterization" of the level of ordinary skill in the art *See* PO Resp. 5–6.

Based on the prior art, the sophistication of the technology at issue, and Dr. Sears' Declaration testimony, we adopt, with minor modification, Petitioner's undisputed definition of the level of ordinary skill. We determine that in this proceeding a person of ordinary skill would have had a bachelor's degree in computer engineering, computer science, electrical engineering, or a related field, with one year of experience in the field of human-machine interfaces and device access security, or an equivalent balance of education and work experience. We have eliminated the open-ended phrase of "at least" in describing the education and experience of a person of ordinary skill. This open-ended description fails to provide the specificity necessary to define the level of ordinary skill.

C. Claim Construction

We construe each claim "using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b)." 37 C.F.R. § 42.100(b) (2021). Under this standard, claim terms are generally given their ordinary and customary meaning as would have been understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005) (en banc) ("We have frequently stated that the words of a claim 'are generally given their ordinary and customary meaning.'" (citations omitted)).

Petitioner states that in the related district court litigation between the parties, the Western District of Texas court entered a Claim Construction

Order on February 10, 2022. (Ex. 1077). Pet. 5. Petitioner also states "the Parties agreed to certain constructions in a Joint Claim Construction Statement" in the Western District of Texas litigation (Ex. 1074). *Id.* Petitioner then proposes that "[f]or purposes of this IPR, Apple applies the District Court's constructions from the *Apple* litigation [Ex. 1077] and constructions agreed to by the Parties (Ex. 1074)[15] that are not otherwise plain and ordinary meaning." *Id.*

Petitioner also highlights specific constructions for the claim terms "database," "conditional access," "biometric signal," and "accessibility attribute" from Exhibits 1074 and 1077. Pet. 6.

Patent Owner proposes "constructions" (1) for the term "accessibility attribute" (PO Resp. 6–7); (2) the phrase requiring a series of entries of the biometric signal "characterised according to at least one of the number of said entries and a duration of each said entry" (*id*. at 7–11); and (3) the "populate" the database limitation concerning enrolling or authorizing new users (*id.* at 11–12).

Patent Owner also provided its views on the differences in claim scope between the term "configured to" and the term "capable of" as used in the challenged claims. *Id.* at 12–14. Petitioner also addresses this topic. Reply 26.

"[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'" *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Ltd.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795,

[15] The cited Exhibits 1074 and 1077 are from the case *prior to* its transfer from the Western District of Texas to the Northern District of California.

803 (Fed. Cir. 1999)). Here, we determine the claim terms that need specific construction are the three terms proposed by Patent Owner for specific construction. Accordingly, we construe these terms below.

1. General Claim Construction Principles

"It is a 'bedrock principle' of patent law that 'the claims of a patent define the invention to which the patentee is entitled the right to exclude.'" *Phillips*, 415 F.3d at 1312 (citations omitted). "[T]here is no magic formula or catechism for conducting claim construction." *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 801, 809 (Fed. Cir. 2021) (quoting *Phillips*, 415 F.3d at 1324). Fortunately, however, there is substantial judicial guidance.

Claim construction requires determining how a skilled artisan would understand a claim term "in the context of the entire patent, including the specification." *Grace Instrument Indus., LLC v. Chandler Instruments Co., LLC*, 57 F.4th 1001, 1008 (Fed. Cir. 2023) (quoting *Phillips*, 415 F.3d at 1313. *Id.* (citation omitted). "[C]laims must be read in view of the specification, of which they are a part." *Id.* (quoting *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 978 (Fed. Cir. 1995) (en banc)). The Specification, or more precisely, the written description, is the "single best guide to the meaning of a disputed term." *Id.* (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)), and "is, thus, the primary basis for construing the claims." *Id.* (citation omitted). Although claim terms are interpreted in the context of the entire patent, it is improper to import limitations from the Specification into the claims. *Phillips*, 415 F.3d at 1323. Thus, we are careful not to cross that "fine line" that exists between properly construing a claim in light of the specification and improperly importing into the claim a limitation from the specification." *Comark Commc'ns., Inc. v. Harris Corp.*, 156 F.3d 1182, 1186 (Fed. Cir.

1998) ("We recognize that there is sometimes a fine line between reading a claim in light of the specification, and reading a limitation into the claim from the specification.").

While certain terms may be at the center of the claim construction debate, the context of the surrounding words of the claim also must be considered in determining the ordinary and customary meaning of those terms. *ACTV, Inc. v. Walt Disney Co.*, 346 F.3d 1082, 1088 (Fed. Cir. 2003).

We also consider the patent's prosecution history. *Phillips*, 415 F.3d at 1317.

In construing the claims, we may also look to available "extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art." *Phillips*, 415 F.3d at 1314 (quoting *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1116 (Fed. Cir. 2004)).

2. "Accessibility Attribute"

In our Decision to Institute this proceeding, we adopted, for purposes of that Decision, Petitioner's unopposed asserted claim construction for "accessibility attribute," which was an "attribute that establishes whether and under which conditions access to the controlled item should be granted." Dec. Inst. 13 (citing Pet. 6 (citing the Texas District Court's claim construction, Exs. 1074, 1077)). We note here that the District Court included the phrase "to a user" at the end of the construed term, which Petitioner did *not* include. The complete construction by the District Court is an "attribute that establishes whether and under which conditions access to the controlled item should be granted *to a user*." Ex. 1077, 2 (emphasis

added). The District Court did not cite any intrinsic or extrinsic evidence to support its construction.

In Patent Owner's Response, Patent Owner acknowledges Petitioner's proposed construction but asserts that "a mere binary decision to grant access to a device does not constitute an 'accessibility attribute.'" PO Resp. 6–7; *see also* Ex. 2013 ¶ 45 (Patent Owner's expert, Dr. Easttom,[16] testimony that the construction of the term "accessibility attribute" in our Decision to Institute this proceeding "requires more than the binary determination of whether to grant access to a controlled item by virtue of the 'under which conditions' language."). Patent Owner also asserts that Petitioner's "position on the 'accessibility attribute' limitation is muddied at best." PO Resp. 14. According to Patent Owner, Petitioner "and its expert appear to argue that 'accessibility attribute' ***can*** be a binary access decision." *Id.* at 15 (citing Paper 1 [Pet.] at 18–20).

Thus, Patent Owner asserts what an "accessibility attribute" is not (it is not a "binary decision"), but fails to assert a construction of what an "accessibility attribute" is.

We do *not* understand Petitioner to be asserting a construction of the term "accessibility attribute" to mean simply a "binary decision" to grant or

[16] Exhibit 2013 is a 36-page declaration from Dr. Easttom. Dr. Easttom earned a D.Sc. degree in Cyber Security, a Ph.D. degree in Technology, and three master's degrees (one in Applied Computer Science, one in Education, and one in Systems Engineering). Ex. 2013 ¶ 7. Dr. Easttom testifies that he has 30 years of experience in the computer science industry including extensive experience with computer security, computer software, and computer networking; that he has authored 37 computer science books; that he has authored over 70 research papers; and that he is an inventor with 25 patents, including patents related to computer networking. His CV (Ex. 2014) provides details of his extensive experience and education.

not grant access to a locked structure or device. Nor did our Decision to Institute adopt such a "binary decision." The construction asserted by Petitioner in this proceeding, and the construction adopted in our Decision to Institute this proceeding, requires "an attribute that establishes *whether and under which conditions* access to the controlled item should be granted." Dec. Inst. 13 (citing Pet. 6 (citing the Texas District Court's claim construction, Exs. 1074, 1077) (emphasis added)).

As we explain in our analysis below, to avoid any confusion of the meaning of "accessibility attribute," we clarify the construction to add the phrase "if any" to modify the "conditions" that may, or may not, be imposed to allow access. Thus, we determine that an "accessibility attribute" is "an attribute that establishes whether and under which conditions, if any, access to the controlled item should be granted." Based on the language of the claims and Specification, the "accessibility attribute" may include only an "access attribute," which is "unconditional." *See* Ex. 1001, 8:29–38 (stating "the accessibility attribute may comprise *one or more of* an access attribute (granting unconditional access)," a "duress attribute," an "alert attribute," and a "telemetry attribute"); *see also id.* at 16:34–44 (unchallenged claim 3 requiring an access attribute, a duress attribute, and an alert attribute).[17]

Notwithstanding Patent Owner's Response that an "accessibility attribute" is not a "binary decision," Petitioner asserts that "[t]he Parties agree to apply the District Court's construction for the claimed 'accessibility attribute.'" Reply 1. Petitioner also states, however, that Petitioner is relying on McKeeth for teaching two accessibility attributes (duress and

[17] To avoid any confusion, we note that an "access attribute" is one specific example of the generic term "accessibility attribute." Ex. 1001, 8:29–38.

alert) even though "the '705 Patent's independent claims only require outputting a single accessibility attribute." *Id.* at 2.

Petitioner clarifies its position on the construction of "accessibility attribute" by further explaining Petitioner's view that "the '705 Patent describes "outputting an accessibility attribute that includes 'access' without any conditions, which satisfies the 'under which conditions' construction component." Reply. 4.

We begin our claim construction analysis with the language used in the claims.

a) Claims

The term "accessibility attribute" appears directly or through dependency in all the challenged claims.

Independent claim 1 includes the following two clauses that refer to an "accessibility attribute":

(1) "a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an *accessibility attribute*;" (Ex. 1001, 16:1–4)[18]; and

(2) "a transmitter configured to emit a secure access signal conveying information dependent upon said *accessibility attribute*" (*id*. at 16:5–7).

These two references merely establish that an "accessibility attribute' is an output access signal based on matching the biometric signal against the authorized user database of biometric signatures. *See id.* at 5:65–6:2 ("Thus for example if the request 102 is the thumb press on the biometric sensor panel 121 then the user database 105 contains biometric signatures for authorised [sic] users against which the request 102 can be authenticated.").

[18] All italicized emphasis of claim language has been added.

These clauses provide no further structure or function of the claimed "accessibility attribute."

Claim 1 also includes a clause stating that "conditional access" to a user is "dependent upon" information in the "accessibility attribute." *Id.* at 16:11–12. This clause does not require or state that there is, or is not, conditional access. It merely states that "conditional access," if any, depends on what information is in the "accessibility attribute." *See id.* at 16:5–7 (stating that the "information" in the "access signal" in claim 1 is "dependent upon" the "accessibility attribute"). Thus, based on the claim language in claim 1, the scope of the "accessibility attribute" is undefined. The only requirement is that it provide access for authorized users.

Claim 3 (not challenged, but still relevant to claim construction), dependent on claim 1, states that "the [authorized user] database of biometric signatures comprises signatures in *at least one of* a system administrator class, a system user class, and a duress class." Ex. 1001, 16:34–37 (emphasis added). Thus, consistent with Petitioner's argument summarized above (*see* Reply 4–5), the system administrator may be the only authorized user in the database. Claim 3 also further defines the "accessibility attribute" as "comprising:

> *an access attribute* if the biometric signal matches a member of the database of biometric signatures;
>
> *a duress attribute* if the biometric signal matches a member of the database of biometric signatures *and said member belongs to the duress class*; and
>
> *an alert attribute* if the biometric signal does not match a member of the database of biometric signatures.

Id. at 16:18–24 (emphases added).

In claim 3, the conditional "duress attribute" applies only if the user is a member of the "duress class" in the database of biometric signatures. There is, however, no requirement that any member of the "duress class" be in the database.

We recognize that the Federal Circuit has held that the plain and ordinary meaning of "at least one of" is "one or more," but that when the phrase is used in a claim, the issue is what "at least one of" is used to modify. *See SuperGuide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 886 (Fed. Cir. 2004). In *SuperGuide*, the court held that, when "[t]he phrase 'at least one of' precedes a series of categories of criteria, and the patentee used the term 'and' to separate the categories of criteria," the phrase connotes a conjunctive list and requires selecting at least one value for each category. *Id.* For example, in *SuperGuide*, the claim phrase "storing at least one of a desired program start time, a desired program end time, a desired program service, and a desired program type" was interpreted as requiring storing at least one desired program start time, at least one desired program end time, and so forth. *Id.* at 884.

Courts have not, however, interpreted *SuperGuide* as setting forth a *per se* rule that the use of "at least one of" followed by "and" necessarily connotes a conjunctive list. *See Fujifilm Corp. v. Motorola Mobility LLC*, Case No. 12–CV–03587–WHO, 2015 WL 1265009, at *8 (N.D. Cal. Mar. 19, 2015) (summarizing cases and noting that "*SuperGuide* did not erect a universal rule of construction for all uses of 'at least one of' in all patents"). In particular, courts have found *SuperGuide* inapplicable when the listed items following "at least one of" are not categories containing many possible values. *See id.*; *see also TQ Delta, LLC v. Comcast Cable Commc'ns, LLC*, No. 1:15–CV–00611–RGA, 2016 WL 7013481, at *8 (D. Del. Nov. 30,

2016) (list following "at least one of" was of parameters to be selected from, not categories). The Board has also distinguished *SuperGuide* on this basis. *See Hewlett–Packard Co. v. MPHJ Tech. Invs., LLC*, Case IPR2013–00309, Paper 9, slip op. at 8 (PTAB Nov. 21, 2013); *Daifuku Co., Ltd. v. Murata Machinery, Ltd.*, Case IPR2015–00083, Paper 63, slip op. at 4–5 (PTAB May 3, 2016); *Apple, Inc. v. Evolved Wireless LLC*, No. IPR2016-01177, 2017 WL 6543970, at *4 (P.T.A.B. Dec. 20, 2017).

Relevant to our inquiry, therefore, is whether the items that follow "at least one of" in the challenged claims of the '705 patent are categories that may have multiple values (such as in *SuperGuide*) or individual parameters having only one value. Here, we think it is clear that the accessibility attributes and the classes of users are individual parameters that apply to individual people.

As noted above, the first user of the disclosed and claimed invention "is automatically categorised as an administrator." Ex. 1001, 10:38–42. This first user may be the only authorized user. Thus, the only database entry for this first user is a "system administrator class" entry that will generate only an "access attribute (granting *unconditional* access)." *Id.* at 8:29–30 (emphasis added). This is not unlikely because the claims are specifically limited to a "controlled item" that is either "a locking mechanism of a physical access structure," or "an electronic lock on an electronic computing device." *See, e.g.*, *id.* at 16:21–23 (claim 1 stating "wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device"). A similar limitation is in each independent claim. The owner of an individual computing device may be the only authorized user of that device, thus having unconditional access as the "administrator."

Claim 3 allows a database of only a first and only user, who is automatically the system administrator. Ex. 1001, 16:34–37 ("the database of biometric signatures comprises signatures in *at least one of* a system administrator class, a system user class, and a duress class" (emphasis added)). There may be no other individuals in the "system user class" or the "duress class."

Claim 3 further limits claim 1 by stating the "accessibility attribute" in claim 1 comprises[19] the three specific attributes stated in claim 3 – "an "access attribute;" "a duress attribute;" and "an alert attribute." This listing in claim 3 establishes a presumption that these three requirements are *not* included in the claimed "accessibility attribute" in claim 1. *Phillips*, 415 F.3d at 1314–15 ("Differences among claims can also be a useful guide in understanding the meaning of particular claim terms. For example, the presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim." (citations omitted)).[20]

---

[19] "[I]n general, a patent claim reciting an apparatus 'comprising' various components merely means that the apparatus 'includ[es] but is not limited to' those components." *Rothschild Connected Devices Innovations, LLC v. Coca-Cola Co.*, 813 F. App'x 557, 562 (Fed. Cir. 2020) (nonprecedential) (citations omitted).

[20] We recognize that the Board "must base its decision on arguments that were advanced by a party, and to which the opposing party was given a chance to respond." *Masimo Corp. v. Apple Inc.*, Nos. 2022-1631 *et al*, slip op. at 8 (Fed. Cir. Sep. 12, 2023 (nonprecedential)) (citing *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016). The parties argued claim construction, but did not discuss specifically claim differentiation as part of their claim construction analysis. Petitioner argued, however, that the claims allowed for "administrator access as an exemplary access without conditions." Reply 4–5. Patent Owner addressed this in its Sur-reply. Sur-

Based on the claim language, the doctrine of claim differentiation, and the analysis above, we determine that an "accessibility attribute," as used in the challenged independent claims means that a user with a biometric signature in the database is given access to the controlled item. As used in the independent claims, there are no other conditions imposed.

Thus, based on the claim language, an "accessibility attribute" is an attribute that establishes whether and under which conditions, if any, access to the controlled item should be granted.

b) Specification

Claims "must be read in view of the specification, of which they are a part." *Phillips*, 415 F.3d at 1315 (citation omitted). "The specification "is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term." *Id.* (citation omitted). Thus, we turn to the Specification for additional guidance on the meaning of the claim term "accessibility attribute."

The Specification states that the "accessibility attribute establishes whether and under which conditions access to the controlled item 111 should be granted to a user." Ex. 1001, 8:26–28. This is the construction adopted in our Decision to Institute this proceeding.

---

reply 22. Our claim construction analysis, as stated in the text, follows controlling procedures from *Phillips*. The parties also were advised that:

> claim construction, in general, is an issue to be addressed at trial. Claim construction will be determined at the close of all the evidence and after any hearing. The parties are expected to assert all their claim construction arguments and evidence in the Petition, Patent Owner's Response, or otherwise during trial, as permitted by our rules.

Dec. Inst. 14.

The Specification further states:

> the accessibility attribute may comprise *one or more of* an *access attribute (granting unconditional access)*, a *duress attribute* (granting access but with activation of an alert tone to advise authorities of the duress situation), an *alert attribute* (sounding a chime indicating that an unauthorised, but not necessarily hostile, person is seeking access, and a *telemetry attribute*, which represents a communication channel for communicating state information for the transmitter sub-system to the receiver sub-system such as a "low battery" condition.

Id. at 8:29–38 (emphases added). Thus, while four different accessibility attributes are disclosed (access attribute, duress attribute, alert attribute, and telemetry attribute), the Specification, consistent with the claims discussed above, states that the disclosed invention "may comprise *one or more of"* these four attributes. Ex. 1001, 8:29–30. The Specification also states that an "access attribute" grants "unconditional access." *Id.* at 8:30.

The term "accessibility attribute" does not appear in the Specification after column 8 until it appears again in the claims.

Thus, based on the Specification, an "accessibility attribute" is an attribute that establishes whether and under which conditions, if any, access to the controlled item should be granted. The term "if any" is required because an "access attribute" grants "unconditional access" (*id.*) and it may be the only attribute included as an "accessibility attribute." *See id.* at 8:29–38 (stating the accessibility attribute "may comprise one or more of*"* the four disclosed specific attributes).

c) Prosecution History

The parties have not directed us to any persuasive evidence from the proceedings leading to issuance of the '705 patent to inform our construction of the term "accessibility attribute."

d) Extrinsic Evidence

The parties do not direct us to any persuasive extrinsic evidence concerning the meaning of the term "accessibility attribute."

e) Claim Construction Conclusion for "Accessibility Attribute"

We recognize that "[t]he very nature of words would make a clear and unambiguous claim a rare occurrence." *Autogiro Co. of Am. v. United States*, 384 F.2d 391, 396 (Ct. Cl. 1967). The Federal Circuit, however, has provided a beacon, which we have followed, to guide us in determining the proper construction when we encounter ambiguities or differing interpretations from the parties:

> Ultimately, the interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim. The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction.

Renishaw PLC v. Marposs Societa' per Azioni, 158 F.3d 1243, 1250 (Fed. Cir. 1998) (citations omitted).

Based on the evidence and the analysis above, we determine that that the term "accessibility attribute" means "an attribute that establishes whether and under which conditions, if any, access to the controlled item should be granted." This is the construction that stays true to the claim language and most naturally aligns with the patent's description of the invention.

3. Biometric Signal Characterised by Number and Duration

All of the challenged claims include a clause that requires receiving, being configured to receive, or being capable of receiving "a series of entries of the biometric signal," where the series is "characterised" or determined by

"at least one of the number of said entries and a duration of each said entry." *See*, Ex. 1001, 16:13–18 (for independent claim 1). We refer to these clauses collectively as the "number and duration" clauses.

These number and duration clauses all go to the embodiment of the invention that allows the administrator to require a biometric input signal that comprises "either or both (a) the number of finger presses and (b) the relative duration of the finger presses." Ex. 1001, 10:60–63 This is the "dit, dit, dit, dah" form of biometric signal discussed in the Specification (*id.* at 11:1–7) and discussed above in this Decision. The capability for an administrator to use this disclosed embodiment exists in the claimed system and method whether the administrator chooses to use it or not.

As stated in the Specification, the administrator may use a single thumb press on a sensor for the required biometric signal. Ex. 1001, 5:60–63 ("for example, if the biometric sensor 121 in the code entry module 103 is a fingerprint sensor, then the request 102 typically takes the form of a thumb press on a sensor panel"). Alternatively, the administrator "can provide control information to the code entry module by providing *a succession of finger presses to the biometric sensor 121*." *Id.* at 10:56–58. Thus, as disclosed in the '705 patent, whether using a single thumb press or a succession of finger presses of variable number and duration, the input vehicle is the same – biometric sensor 121.

Patent Owner asserts that Petitioner, and the Board in its Decision to Institute this proceeding, improperly "blur the lines" between "'knowledge-based' security features (those based on knowledge, such as a passcode or particular pattern, and not on any attribute of the user), and a biometric signal based on the unlearnable attribute of the user." PO Resp. 9. We

disagree. Patent Owner fails to properly understand Petitioner's, and our, analysis of the number and duration clauses.

Patent Owner asserts:

> Crucially, the antecedent for this series is 'a series of entries of the biometric signal,' *i.e.*, the entries and corresponding series are 'of the biometric signal,' and the 'number of said entries and a duration of each said entry' refers to the entries of the biometric signal, and not an entry of some other information, such as knowledge-based information.

Id. at 9. As explained above, in our Decision to Institute, and in this Decision, we construe the number and duration clauses to require a number and duration of biometric signals because the input for these biometric signals is a biometric sensor, as disclosed in the Specification. A fingerprint sensor's ability to recognize a fingerprint is not turned off when a succession of finger presses is applied to the fingerprint sensor. Thus, contrary to Patent Owner's argument (*see* PO Resp. 10), our construction of the number and duration clauses is not based on a "knowledge-based security feature."

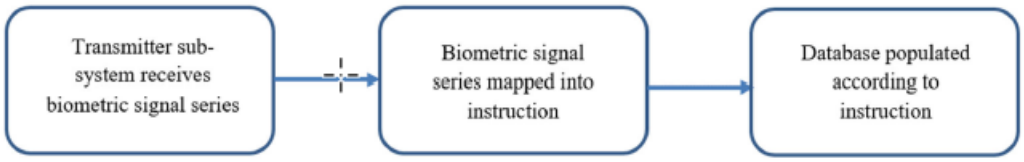
In summary, our construction of the number and duration clauses is that the number and/or duration of entries is based on entries of a biometric signal, such as a finger press on a fingerprint sensor. Based on the claim language and the Specification (*see* Ex. 1001, 10:61–63 ("the control information is encoded by *either or both* (a) the number of finger presses and (b) the relative duration of the finger presses") (emphasis added)), this is the construction that stays true to the claim language and most naturally aligns with the patent's description of the invention.

4. Populate the Database

Patent Owner asserts that if and when the number and duration clause (citing clause 1(d)(1) in Petitioner's Claim Listing Appendix (Pet. 64)) is

used by an administrator to establish an authorized user, that information is "mapped into an instruction and the resulting instruction is used to populate the database of biometric signatures." PO Resp. 11 (citing representative clauses 1(d)(2) and 1(d)(3) from Petitioner's Claim Listing Appendix). Patent Owner also acknowledges that "the 'populate' limitation in claim 1 is part of that enrolling feature." PO Resp. 11. We understand that reference to the "enrolling" feature is a reference to the administrator establishing a database of authorized users ("biometric signatures") that will be used to match against a received biometric signal to provide access to the controlled item dependent upon the success or otherwise of the matching operation. *See, e.g.* claim 12.

Patent Owner asserts that "[t]o satisfy the requirements for antecedent claiming, 'said series' in clause 1(d2) must refer to the 'series of entries of the biometric signal' in clause 1(d1)." PO Resp. 11. Patent Owner provides the following flow diagram for populating the database:



Id. at 12 (citing Ex. 2011 ¶ 82). The flow diagram provides Patent Owner's graphic interpretation of the three steps involved in populating the database of approved users. These basic steps apply whether the biometric signal is a single finger press or a series of finger presses.

In its claim construction arguments, Patent Owner attempts to draw a sharp distinction between a process using a single finger press, and a process that uses the number and duration of finger presses, as two technologically distinct processes. Patent Owner has not, however, cited any persuasive

evidence to support this asserted distinction. In fact, the evidence is to the contrary.

As we have noted throughout this claim construction analysis, the controlling case law is consistent in stating that the Specification is the single best guide to the meaning of a disputed term, and is, thus, the primary basis for construing the claims. *E.g.*, *Grace Instrument*, 57 F.4th at 1008. In the '705 patent, the Specification also is consistent in stating that the using a number and duration of finger presses as a biometric input signal, and using a single finger press, are done exactly the same way – both use the same biometric fingerprint sensor. *See, e.g.*, Ex. 1001, 10:56–58 (the administrator "can provide control information to the code entry module by providing a succession of finger presses *to the biometric sensor 121*"**)** (emphasis added).

The Specification also is consistent in stating that the system administrator establishes a database of authorized users, or authorized biometric signatures, by using appropriate software to create, or populate, the database. *See, e.g.*, *id.* at 14:27–37.[21] There is no persuasive evidence to which we have been directed that the biometric fingerprint sensor ceases to

[21] The cited text from the Specification states:

> FIG. 10 is a schematic block diagram of the system in. FIG. 2. The disclosed secure access methods are preferably practiced using a computer system arrangement 100', such as that shown in FIG. 10 wherein the processes of FIGS. 3–4, and 6–9 may be implemented as software, such as application program modules executing within the computer system 100'. In particular, the method steps for providing secure access are effected by instructions in the software that are carried out under direction of the respective processor modules 107 and 109 in the transmitter and receiver sub-systems 116 and 117.

function as a biometric fingerprint sensor when the administrator establishes a database using the number and duration of finger presses. Patent Owner's argument is actually to the contrary in that Patent Owner asserts that the number and duration of finger presses is a biometric signal. PO Resp. 9 ("[T]he entries and corresponding series are 'of the biometric signal,' and the 'number of said entries and a duration of each said entry' refers to the entries of the biometric signal, and not an entry of some other information, such as knowledge-based information."). This means the number and duration of entries must include a biometric component.

If the number and duration of presses did not include a biometric component, it would be simply a "knowledge-based" security measure, based on a pattern rather than based on a unique physical attribute of the user. Patent Owner asserts that such a pattern can be learned, and thus is inconsistent with the '705 patent's claims and disclosure. PO Resp. 7–11. Whether the software used by the administrator to populate the database of approved users relies on this biometric component is not disclosed in the '705 Specification.

We now turn to the merits of Petitioner's asserted Grounds of unpatentability.

D. Ground 1
Claims 1, 4, 6, 10–12, 14–17
Based on Mathiassen, McKeeth, and Anderson

Petitioner contends that claims 1, 4, 6, 10–12, and 14–17 would have been obvious over the combination of Mathiassen, McKeeth, and Anderson. Pet. 9–54.

1. Mathiassen (Ex. 1004)

We make the following finding of facts concerning Mathiassen.

Rather than using passwords or "tokens," such as an entry card, Mathiassen discloses a portable fob-type fingerprint sensor to access secured items, such as vehicles, computers, safes, medicine cabinets, and weapons cabinets. Ex. 1004 ¶¶ 1–4, 16–18, 109–113.

Figure 8 from Mathiassen is reproduced below.

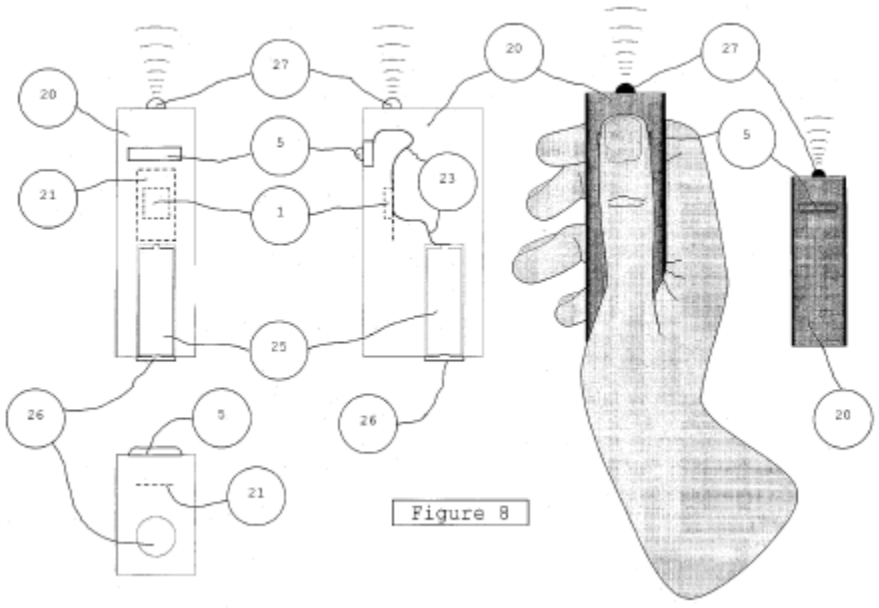


Figure 8 is a schematic illustration of a "user input device" providing access to a vehicle door. As shown in Figure 8, portable device 20 contains fingerprint sensor 5 coupled to a miniature printed circuit board 21 on which is mounted integrated circuit ("IC") 1. Ex. 1004 ¶ 147. Thus, remote control 20 becomes a biometric sensor. *Id.* ¶ 5. Remote biometric control 20 includes battery 25 as a power supply. *Id.* ¶ 147. Battery 25 is connected to printed circuit board ("PCB") 21 by wires. *Id.*

Remote biometric control 20 also is equipped with wireless 2-way transceiver 27. All the active components are connected to integrated circuit 1 by cables 23 through printed circuit board 21. *Id.*

Ignition control device 15 (*see* Fig. 6) is mounted inside the car on gear stick 71 or on steering wheel 72. *Id.* ¶ 148. Remote control 20 and embedded ignition control 15 are both connected to a central computer (not shown) in the car. *Id.* ¶ 149. Remote control 20 is connected to the central computer by 2-way wireless transceiver 27, while ignition control 15 is hard-wired to the central computer. *Id.*

2. McKeeth (Ex. 1005)

We make the following finding of facts concerning McKeeth.

McKeeth discloses a method and system for authenticating a user to access a computer system. Ex. 1005, Abstr.

McKeeth summarizes the problems with current systems for accessing computers, such as using a private identification code or password (Ex. 1005, 1:14–30),[22] or a machine readable card (*id.* at 1:31–36). McKeeth also notes that "some computer makers considered using the user's fingerprint to authenticate and grant access to the computer system." *Id.* at 1:36–38. McKeeth recognized, however, that even using fingerprints was not without problems because "a sophisticated computer hacker may be able to copy the user's fingerprint and provide a simulated signal to the computer system to obtain access." *Id.* at 1:51–54.

The method and system disclosed in McKeeth provide for one or more of various types of user inputs to be used, alone or in combination, for authentication. These various inputs can be a password, a unique series of clicks of a mouse, a unique geometric pattern created by the user (*see* Figs. 3A–3D (illustrating a simple triangle, rectangle, line, or circle drawn by the

[22] Citations are to column:line of McKeeth.

user), an audio sensor (for voice recognition), or an optical scanner for fingerprint, retina scans, or other biometric inputs. Ex. 1005, 2:2:53–3:12.

Figure 1 from McKeeth is reproduced below.

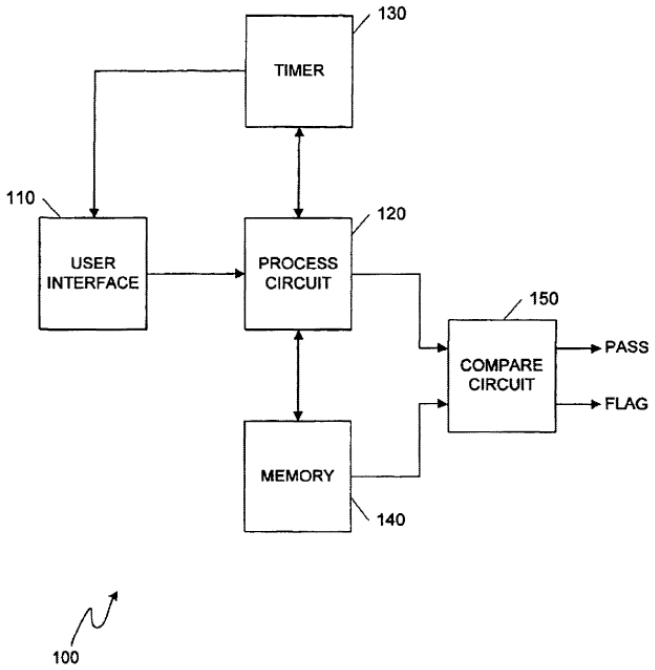


Figure 1 from McKeeth is a block diagram showing one version of a the method and system for authenticating the identity of a user disclosed in McKeeth. Ex. 1005, 2:36–37. As shown in Figure 1, computer system 100 includes user interface 110 that is operationally connected to process circuit 120. *Id.* at 2:55–57. User interface 110 may be any input device that is used to enter or communicate information to computer system 100, such as a keyboard, mouse, trackball, pointer, touch-screen, remote terminal, audio sensor, optical scanner, telephone, or any similar user interface. *Id.* at 2:57–61.

Process circuit 120 is configured to receive input signals from user interface 110. The process circuit is operationally connected with timer 130 that measures time duration between the various input signals. Ex. 1005,

3:36–38. If, for example, the user performs a fingerprint scan and/or pattern within the designated time, process circuit 120 communicates the input signals to compare circuit 150 for authentication. *Id.* at 3:52–55. Compare circuit 150 is operationally coupled to memory 140, which stores a list of legitimate user identifications (ID's) with respective passwords, fingerprint, pattern, or any other type of security information for recognition by the computer system. *Id.* at 3:55–60. If there is a match between the user inputs, within the designated time, and stored security information, the compare circuit 150 issues a "pass" signal to computer system 100. *Id.* at 65–67.

3. Anderson Ex. (1006)

We make the following finding of facts concerning Anderson.

Anderson also discloses a system and method for authenticating an authorized user to access a secured device. Anderson's disclosed system inputs an access code "via temporal variations in the amount of pressure applied to a touch interface." Ex. 1006, Abstr.

Anderson's method of inputting an access code uses digitizer pad 120 as a touch interface, which may include an optical scanner or thermal sensor for collecting an image of the user's fingerprint. Ex. 1006, 5:43–44, 7:4–7. The user enters the access code as a series of pressure pulses having varying durations. *Id.* at 6:45–47. This fingerprint access code is then compared with a stored code template to determine whether they match. If they do, access is permitted. *Id.* at 6:48–54.

Anderson discloses a system where the touch interface may sense only "temporal applications of pressure," relying on *timing* of the pressure applications for entry of the access code. Ex. 1006, 7:28–30; Fig. 4A. Alternately, as shown in FIG. 4B, the touch interface may sense both

temporal applications of pressure and variations in pressure magnitude or intensity. *Id.* at 7:34–37. Thus, the access code would be entered as a series of alternating short and long pressure applications that vary both in duration and magnitude. *Id.* at 7:37–39.

Annotated Figure 4A from Anderson is reproduced below.

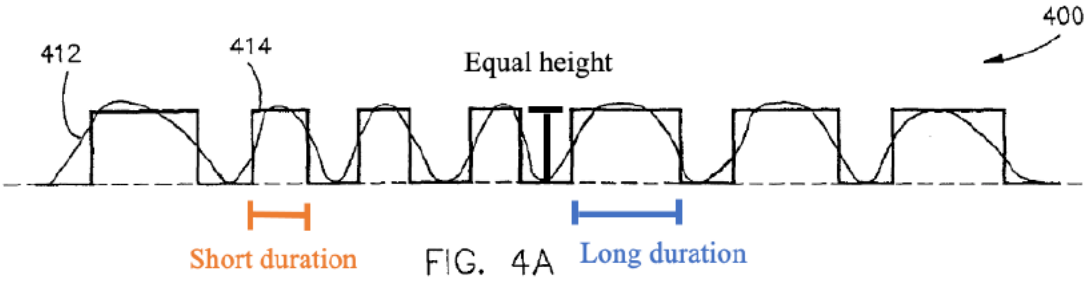


FIG. 4A

Figure 4A from Anderson is a diagram illustrating entry of an access code via temporal pressure variation. Ex. 1006, 2:65–67. The annotations are provided by Dr. Sears in his declaration testimony. Ex. 1003 ¶ 100. As explained by Dr. Sears, in Figure 4A, "the height of each bar the same because the magnitude or intensity of the finger pressure press is not detected. However, at least some of the presses have a different duration than other presses, as represented by the width of each bar." *Id.*

Annotated Figure 4B from Anderson is reproduced below.

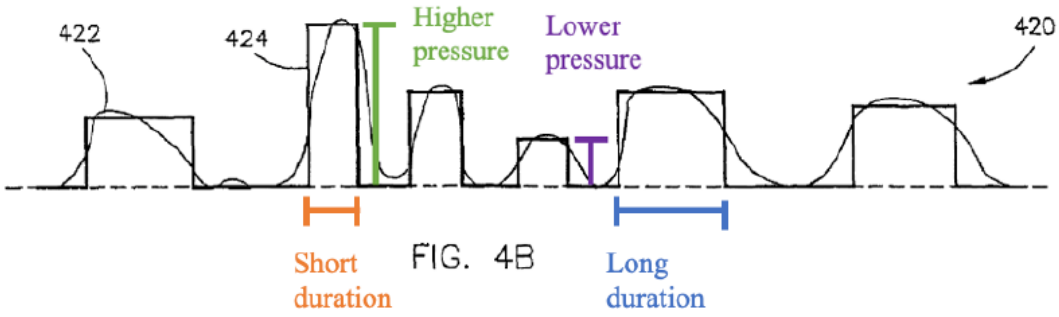


FIG. 4B

Figure 4B from Anderson is a diagram illustrating entry of an access code via temporal pressure variation. Ex. 1006, 2:65–67. The annotations are provided by Dr. Sears in his declaration testimony. Ex. 1003 ¶ 101. As

explained by Dr. Sears, Figure 4B "illustrates variations in both the amount of pressure applied using the height of each bar and the duration of the applied pressure using the width of each bar." *Id.*

We begin our claim analysis with claim 1.

4. Analysis of Independent Claim 1

Petitioner provides a clause-by-clause analysis of independent claim 1, identifying where in each of the cited references, Mathiassen, McKeeth, or Anderson, the claimed element is disclosed, and why it would have been obvious to a person of ordinary skill to combine the various disclosed elements with a reasonable expectation of success. *See* Pet. 9–42. Throughout its analysis, Petitioner cites the Declaration testimony (Ex. 1003) of Dr. Sears for evidentiary support. [23] In general, Petitioner explains the proposed combination of references as:

> First, Mathiassen's biometric security system is modified to output a duress and/or alert condition, per McKeeth, responsive to a user's biometric signature. Mathiassen already contemplates outputting various commands based on different user-inputted biometric signals, indicating a duress and/or alert condition based on a particular inputted biometric requires only simple programming. Second, Mathiassen is modified to recognize a touch duration, per Anderson, of the fingerprint representation on the fingerprint sensor.

Reply 1.

For ease of reference and consistency, we will refer to Petitioner's Claim Listing Appendix convention (Pet. 64–69), as did Patent Owner (*see, e.g.*, PO Resp. 11 referring to "transmitter subsystem (representative

[23] Petitioner cites this testimony as "Dec." Pet. 3, fn 1. We will cite it, as we do all other evidence, by reference to its Exhibit number, which is Exhibit 1003.

clause 1(d1)), that series is mapped into an instruction (representative clause 1(d2)), and the resulting instruction is used to populate the database of biometric signatures (representative clause 1(d)(3))").

Patent Owner asserts that Petitioner has not met its burden to prove unpatentability because:

(1) Mathiassen, alone or in combination with other references, does not disclose the "accessibility attribute" limitation, as properly construed, and, moreover, there is no motivation to combine Mathiassen with the other references (PO Resp. 14–25);

(2) Anderson, alone or combined with Mathiassen, does not disclose the "biometric signal duration limitation," and, also, there is no motivation to combine Anderson and Mathiassen (*id.* at 26–32);

(3) the references, alone or in combination, do not "populate" the database according to an "instruction" (*id.* at 32–35); and

(4) there were simpler solutions available to a skilled person than the Mathiassen/Anderson combination (*e.g.*, PO Resp. 3–4, 24–25, 30–31; Sur-reply 6–17).

Patent Owner states these same arguments apply to independent claims 10, 11 and 14–17, as well as the challenged dependent claims. PO Resp. 35 (asserting that these claims "contain the 'populating,' 'duration,' and 'accessibility attribute' limitations, and, as the prior art cited by Apple does not teach these limitations, the cited prior art does not render these [ ] claims obvious as a result thereof").

Patent Owner's defenses are based in large part on accepting Patent Owner's asserted claim constructions, which we have *not* done.

a) Preamble
"A system for providing secure access to a controlled item"

Petitioner asserts that "[t]o the extent the preamble is limiting, Mathiassen teaches a system for providing secure access to a controlled item." Pet. 9 (citing Mathiassen, Abstr., ¶¶ 16, 122–123, 145–147; Ex. 1003 ¶¶ 112–113).

Patent Owner does not contest specifically Petitioner's arguments with respect to the preamble of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests the preamble of claim 1.

b) Clause 1(a)
"a memory comprising a database of biometric signatures"

Petitioner asserts that Mathiassen discloses a stored database of tables stored in memory 7, 7A. Pet. 11–13 (citing Ex. 1004, ¶¶ 50, 147, Fig. 2B; Ex. 1003 ¶¶ 119–121).

Patent Owner does not contest specifically Petitioner's arguments with respect to the preamble of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests the claimed memory of a database of biometric signatures.

c) Clause 1(b)
"a transmitter sub-system"

Petitioner asserts Mathiassen teaches a transmitter subsystem, including transceiver 27, fingerprint sensor 5, processor 2 (of integrated circuit 1), and non-volatile memory 7, 7A, each housed in portable control 20. Pet. 13–14 (citing Ex. 1004 ¶¶ 185–188; Ex. 1003 ¶¶ 123–126).

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(b).

d) Clause 1(b1)
"a biometric sensor configured to receive a biometric signal"

Petitioner asserts that Mathiassen's "fingerprint sensor 5" is a "biometric sensor for receiving a biometric signal" because it detects a finger on the sensor and processes raw images of fingerprints. Pet. 14 (citing Ex. 1004 ¶ 49; Ex. 1003 ¶¶ 127–128).

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(b1).

e) Clause 1(b2)
"a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute"

As discussed in detail in Section II.C.2 (Claim Construction), the term "accessibility attribute" is an "attribute that establishes whether and under which conditions, if any, access to the controlled item should be granted to a user." Thus, the attribute may, or may not, impose any conditions on permitting access.

Petitioner asserts "Mathiassen's processor 2 of the IC 1 in the portable door control 20 discloses a "transmitter sub-system controller," as recited in

claim 1. Pet 15. According to Petitioner, Mathiassen's portable control processor is configured to match the user's biometric signal against the database of biometric signatures. Pet. 16 (citing Ex. 1003 ¶¶ 131, 133–135). If there is a match, the processor will proceed to open (or lock) the car doors. *Id.* at 17 (citing Ex. 1004, ¶¶ 180–182); Ex. 1003 ¶ 136).

Petitioner also asserts Mathiassen's "open door" command as modified by McKeeth's "teaching of duress and alert conditions" discloses "or renders obvious" outputting an accessibility attribute, as claimed. Pet. 17 (citing Ex. 1003 ¶¶ 137–171).

Petitioner also asserts that McKeeth discloses a system in which "access is granted where 'there is a match between the input and security information.'" Pet. 18 (citing Ex. 1005, 3:65–67, 3:11–28). McKeeth discloses different types of input security information, including audio sensors to detect a voice recognition and an optical scanner for fingerprint and/or retina scans. Ex. 1005, 3:1–10. Any, a combination, or all of the described types of input signals may be used to authenticate a user. Ex. 1005, 3:11–12. If the input and security information do not match the stored information, the compare circuit issues a "flag signal" indicating denial of access by the user. *Id.* at 4:2–4.

Petitioner concludes that the "collective teachings" of Mathiassen and McKeeth:

> teach outputting an accessibility attribute, where the accessibility attribute may be one of an access attribute (Mathiassen and granting access to a car owner/administrator), a duress attribute (McKeeth and granting limited access along with a security alert), and an alert attribute (McKeeth and denying access along with a security alert).

Pet. 21–22 (italic font for reference names deleted throughout herein). Thus, Mathiassen combined with McKeeth suggests a more comprehensive "accessibility attribute" than Mathiassen alone.

As discussed above, Petitioner's position is that an "accessibility attribute" without any conditions satisfies the 'under which conditions' construction component." Reply 4. Based on our claim construction of "accessibility attribute, we agree with Petitioner's position.

Petitioner concludes that Mathiassen and McKeeth "each teaches **under what conditions** access is granted." Pet. 18. "Specifically, both references teach outputting an accessibility attribute upon there being a match of a live or access biometric signal to a stored biometric signal." *Id.* Petitioner notes that McKeeth "teaches both a duress instruction and an alert instruction when there is no match." *Id.*

Petitioner also provides reasoning why it would have been obvious to combine Mathiassen and McKeeth with a reasonable expectation of success. Pet. 22–24. According to Petitioner, it would have been obvious to a person of ordinary skill, that is a person with a degree in computer engineering, computer science, electrical engineering, or a related field, and with one year of relevant experience, to increase user safety of Mathiassen by providing accessibility attributes indicating duress access or alert access, as proposed in McKeeth, to thereby increase user security. *Id.* (citing Ex. 1003 ¶¶ 149, 151–161).

Patent Owner asserts that Mathiassen and McKeeth disclose only a "binary" system, without specifying the conditions under which access is permitted. PO Resp. 14–17. We disagree based on our analyses above. Our construction of the "accessibility attribute" allows for conditional access, if

any conditions are imposed, or unconditional access, if no conditions are imposed. Patent Owner's arguments fail to account for this construction.

Patent Owner also argues that there is no motivation to combine Mathiassen and McKeeth because there were simpler alternative solutions available, the existence of which undermines the motivation to combine. PO Resp. 19–23; Sur-reply 4–8. This argument is inconsistent with controlling caselaw that makes clear "[i]t's not necessary to show that a combination is the *best* option, only that it be a *suitable* option." *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1380 (Fed. Cir. 2023) (citing *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 784, 800 (Fed. Cir. 2021) (quoting *PAR Pharm., Inc. v. TWI Pharms., Inc.*, 773 F.3d 1186, 1197–98 (Fed. Cir. 2014) (emphasis in original)); *see also Netflix, Inc. v. DivX, LLC*, No. 2022-1083, 2023 WL 2298768, at *5 (Fed. Cir. Mar. 1, 2023) (citing *In re Mouttet*, 686 F.3d 1322, 1334 (Fed. Cir. 2012) and *In re Kahn*, 441 F.3d 977, 990 (Fed. Cir. 2006)).

The motivation-to-combine analysis is a flexible one. "*[A]ny* need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *KSR*, 550 U.S. at 420 (emphasis added). And "[a] person of ordinary skill is also a person of ordinary creativity, not an automaton." *Id.* at 421. Thus, "in many cases[,] a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle." *Id.* at 420. The motivation-to-combine analysis "need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court [or this Board] can take account of the inferences and creative steps that a person of ordinary skill in the art would employ." *Id.* at 418.

Here, based on our claim construction and analysis of the references, we determine that Petitioner establishes the claimed "accessibility attribute."

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(b2).

f) Clause 1(b3)

"a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute"

Petitioner asserts Mathiassen teaches a "transmitter," namely transceiver 27 of portable control 20, that is "configured to emit a secure access signal conveying information dependent upon said accessibility attribute." Pet. 24 (citing Ex. 1004 ¶¶ 147, 186; Ex. 1003 ¶¶ 172–173).

Petitioner also asserts the IC processor in Mathiassen encrypts a command, such as "open door," with a temporary password or key. Pet. 25 (citing Ex. 1004 ¶¶ 50, 185). Transceiver 27 wirelessly transmits the encrypted command to a transceiver at the central car computer. *See* Ex. 1004 ¶¶ 186–188); Ex. 1003 ¶ 178. Petitioner concludes that "[b]ecause Mathiassen teaches the key used to encrypt the command sent from the portable control to the ignition control/car computer changes for each transaction, the encrypted command is non-repeatable and non-replayable. Therefore, Mathiassen teaches a 'secure access signal.'" Pet. 26 (citing Ex. 1003 ¶¶ 182–183).

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(b3).

g) Clauses 1(c and 1(c1))
"a receiver sub-system comprising: a receiver sub-system controller configured to: receive the transmitted secure access signal"

Petitioner discusses clauses 1(c) and 1(c1) together, and we follow this format.

Petitioner asserts Mathiassen teaches a receiver sub-system comprising "the central car computer and door lock transceivers, the central car computer, and ignition control 15." Pet. 28 (citing Ex. 1004 ¶¶ 186–188). As asserted by Petitioner, the central car computer includes a transceiver receiving the secure access signal (the "open door" command) from the portable control. *Id.* As Petitioner states correctly "the door locks include a transceiver receiving the relayed and authenticated open door command." Pet. 28. (citing Ex. 1003 ¶¶ 187–189; Ex. 1004 ¶¶ 149, 167, 186–187). According to Petitioner, a "transceiver" is well understood to include a receiver. *Id.* (citing Ex. 1003 ¶ 190). Petitioner concludes that Mathiassen discloses a receiver sub-system, as claimed. *Id.* (citing Ex. 1003 ¶ 191).

Petitioner also asserts that Mathiassen discloses a receiver sub-system, including the transceivers, the central car computer, and ignition control. Pet. 28–30. According to Petitioner, "a POSITA would have understood a processor performing the claimed function of receiving the signal and providing conditional access," which is "at least equivalent to the claimed "controller." *Id.* at 28 (citing Ex. 1003 ¶¶ 192–197).

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests clauses 1(c) and 1(c1).

h) Clause 1(c2)
"a receiver sub-system control . . . configured to: provide conditional access to the controlled item dependent upon said information"

Petitioner's proposed construction in this proceeding for the phrase "conditional access" is "access based on accessibility attributes." Pet. 6, 30; *see also* Ex. 1074, 3 (the Joint Claim Construction Statement in the related parallel litigation). We have defined the term "accessibility attribute" above and discussed its application in previous clauses. We need not repeat this analysis.

Petitioner asserts Mathiassen discloses access to a closed item, such as a door, dependent upon the information in the secure access signal. Pet. 30. According to Petitioner, because Mathiassen's commands specifically instruct a function (i.e., open door locks vs. lock door locks), the command (i.e., the "secure access signal") includes information specific to the instructed function. *Id.* (citing Ex. 1004 ¶ 167; Ex. 1003 ¶ 200).

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests clauses 1(c2).

i) Clause 1(d)
"wherein the transmitter sub-system controller is further configured to:"

Similar to the analysis for clause 1(b2) discussed above, Petitioner asserts that "processor 2 of IC 1 in [the] portable door control" in

Mathiassen discloses this element. Pet. 31 (citing Ex. 1004 ¶¶ 50, 147; Ex. 1003 ¶ 202).

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests clauses 1(d).

j) Clause 1(d1)
"[configured to] receive a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;"

Petitioner acknowledges that [a]lthough Mathiassen teaches inputting a command via a series of fingerprint representations, Mathiassen does not teach determining a duration of each entry. Anderson teaches inputting an access code including fingerprint presses of varying duration." Pet. 3.

Petitioner asserts Mathiassen discloses storing "a series of consecutive fingerprint representations generated by the fingerprint sensor signal capture and preprocessing block (5C))" that represent various "finger movements across the sensor in two dimensions." Pet. 32 (citing Ex. 1004 ¶ 192; Ex. 1003 ¶¶ 205–210).

Petitioner relies on Anderson for the disclosure of a "series of fingerprint pressure pulses of varying duration. Pet. 33–34 (citing Ex. 1006, 6:45–48 ("For example, wherein the access code is entered by the user as a series of pressure pulses having varying durations, a predetermined tolerance may be provided for variations in the lengths of the pulses."), 7:40–47); *see also id.* at 7:34–39 (disclosing that, "as shown in FIG. 4B, the touch interface may sense both temporal applications of pressure and variations in pressure magnitude or intensity. Thus, the access code would be entered as

a series of alternating short and long pressure applications that vary both in duration and magnitude")).

As we explained above in our discussion of Anderson, there can be no reasonable dispute that Anderson discloses input biometric signals that vary in number and duration.

As explained by Petitioner,

> In Mathiassen, the series of directional finger movements instruct a particular command. A POSITA would have found it obvious to substitute or modify such directional finger movements with a series of presses of varying duration, as taught by Anderson, for instructing a command at portable device 20.

Pet. 36 (citations omitted).

Petitioner also provides argument and probative evidence as to why a person of ordinary skill would have combined the disclosures of the references, with a reasonable expectation that the combination would be successful. Pet. 35–36. As explained by Petitioner,

> There would have been a reasonable expectation of success in modifying Mathiassen's processor 2 in control 20, because it executes software and directs hardware for detecting and categorizing directional movement and touch/no touch. Mathiassen's processor is already operable to detect a finger press because it receives the fingerprint representations, in the form of captured raw images, from the fingerprint sensor. *Id.* The modification therefore only requires simple programming techniques (e.g., modification of the disclosed translation program to count the number and duration of a "touch" or "no touch") that were within a POSITA's expertise.

Id. at 37 (citing Ex. 1004 ¶ 192; Ex. 1003 ¶¶ 224–225).

Patent Owner asserts that the "pressure pulses" in Anderson do not generate biometric signals because they are captured "as the pressure code is entered," and are therefore not part of the pressure code itself. *See* PO

Resp. 27. Patent Owner also explains that "combining Mathiassen's fingerprint sensor with Anderson's pressure code does not produce the claimed invention, as any duration would apply to a nonbiometric signal." *Id.* at 28 (citing Ex. 2013 ¶¶ 69–71). Dr. Easttom testifies that Anderson does not capture a biometric signal. Ex. 2013 ¶¶ 69–71.

Petitioner, however, relies on Mathiassen and McKeeth for the biometric sensing, but also relies on Anderson, which suggests the benefits and options of using a number and duration of pulses as inputs. Reply 1. As explained by Petitioner,

> First, Mathiassen's biometric security system is modified to output a duress and/or alert condition, per McKeeth, responsive to a user's biometric signature. Mathiassen already contemplates outputting various commands based on different user-inputted biometric signals, indicating a duress and/or alert condition based on a particular inputted biometric requires only simple programming. Second, Mathiassen is modified to recognize a touch duration, per Anderson, of the fingerprint representation on the fingerprint sensor.

Id.

Because Mathiassen, like the '705 patent, uses a biometric sensor as the input device, it will detect the biometric part of the input signal, while also sensing the number and duration of inputs.

Dr. Sears' annotated figures 4A and 4B from Anderson (*see* Ex. 1003 ¶¶ 97, 98; also discussed in Section II.D.3 of this Decision) are reproduced again below for convenient reference.

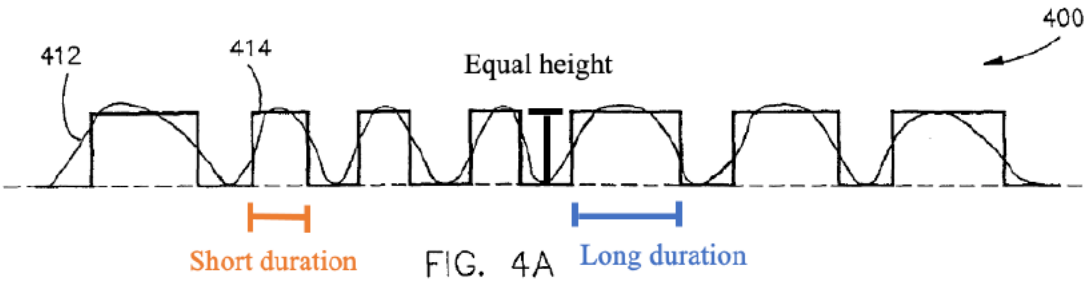


FIG. 4A

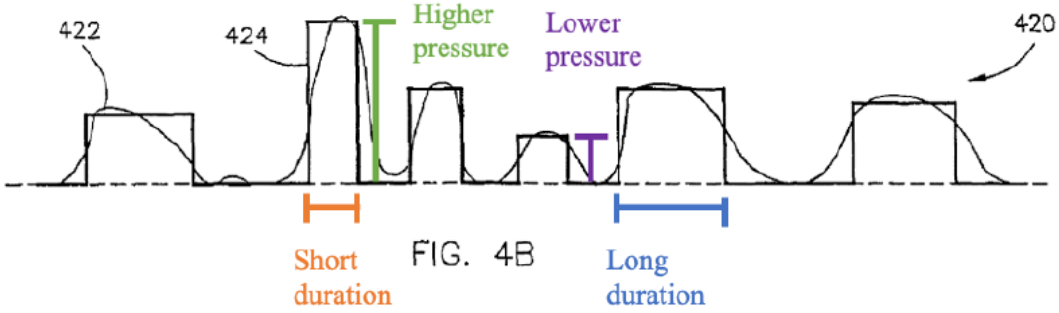


FIG. 4B

Dr. Sears testifies that Anderson's method of inputting an access code uses digitizer pad 120 as a touch interface, which may "include an optical scanner or thermal sensor for collecting an image of the user's fingerprint. Ex. 1003 ¶ 96 (citing Ex. 1006, 5:43–44, 7:4–7). The user then enters the access code "as a series of pressure pulses having varying durations." *Id.* (quoting Ex. 1006, 6:45–47). This fingerprint access code is then compared with the "stored code template" in Anderson to determine a "match" to enable the desired function. *Id.* (citing Ex. 1006, 6:48–54). Dr. Sears testifies that "Anderson teaches two different access code applications: one where both the pressure of each press *and* the duration of each press is detected (Fig. 4A), and another where only the duration of each press is detected (Fig. 4B)." *Id.* (citing Ex. 1006, 7:28–39).

Dr. Sears also states, "Anderson discloses that in the second option, the 'access code would be entered as a series of alternating pressure applications of varying duration' where the touch interface 'may only sense temporal applications of pressure' and "not detect variations in pressure

magnitude or intensity." Ex. 1003 ¶ 96 (citing Ex. 1006, 7:28–34, discussing Figure 4A in Anderson). It is Dr. Sears' opinion that "in the first [option] the touch interface may sense both temporal applications of pressure and variations in pressure magnitude or intensity." *Id.* (citing Ex. 1006, 7:34–37, discussing Fig. 4B in Anderson).

Patent Owner asserts that a "simpler combination" was available. PO Resp. 30; Sur-reply 4–8. According to Patent Owner, "a simpler solution would have been to add Anderson's pushbutton to Mathiassen's key fob." PO Resp. 30 (citing Ex. 2013 ¶ 77). However, as explained above, "[i]t's not necessary to show that a combination is the *best* option, only that it be a *suitable* option." *Intel Corp.*, 61 F.4th at 1380 (citations omitted).

Based on the Petitioner's arguments and evidence summarized above, we determine Petitioner has sufficiently shown that the cited references, as combined by Petitioner, disclose or suggest limitation 1(d1).

k) Clause 1(d2)
"[the transmitter sub-system controller is further configured to:] map said series [of entries of the biometric signal] into an instruction"

Petitioner asserts Mathiassen discloses the processor in integrated circuit 1 maps the series of biometric signal entries into an instruction by translating the series of finger movements to a command in a command table. Pet. 37–38 (citing Ex. 1004 ¶ 192). The cited disclosure in Mathiassen states:

> As an additional safety feature the portable or embedded device could be equipped with means for the input of code or commands. This is achieved by defining a fingerprint storage segment in non-volatile memory (7, 7A or 7E) where the device may store a series of consecutive fingerprint representations generated by the fingerprint sensor signal capturing and pre-processing block (5C). *Movement analyzing means, in the form*

> *of a hardware or a software movement analyzing program module analyzes the obtained series of fingerprint representations to obtain a measure of the omni-directional finger movements across the sensor in two dimensions. Translation means in the form of a hardware or a software translation program module analyzes and categorizes the omni-directional finger movements across the fingerprint sensor according to predefined sets of finger movement sequences* including directional and touch/no-touch finger movement sequences. *A command table is used to translate the categorized finger movements into control signals whereby the translating means generates control signal for controlling the device, e.g. the stand-alone appliance, in response to the finger movements on the sensor.*

Ex. 1004 ¶ 192 (emphases added). There can be no reasonable dispute that Mathiassen discloses a computer implemented software translation program for converting finger movements into control signals.

l) Clause 1(d3)
[the transmitter sub-system controller is further configured to:] populate the data base according to the instruction

Petitioner asserts the cited references "teache[ ] or render[ ] obvious a system enrolling or populating a database of new users." Pet. 38–42 (citing Ex. 1004 ¶¶ 71, 131, 162–167, 192; Ex. 1003 ¶¶ 231, 236–238, 241–245). Petitioner explains the mapping or the previous clause, and the "populating" of this clause as follows:

> Mathiassen teaches mapping "said series" into an instruction by translating the series of movements obtained from the series of fingerprint representations into a command using the command table. (Paper 1, 37-38; Ex. 1003, ¶¶ 226-230). Mathiassen also teaches enrolling new users by generating master minutiae tables and storing the tables in memory 7,7A. (Paper 1, 38; Ex. 1003, ¶¶ 231, 233-238). Mathiassen-Anderson renders obvious populating the database according to the instruction mapped from the "said series," as a POSITA would have found it obvious to include an enrollment command in the command table.

> (Ex. 1004, [0192]; Ex. 1003, ¶¶ 233-246, pinpoint at ¶ 241). Thus, the administrator's input series of finger movements is mapped into an instruction, i.e., an instruction to enroll a user. (Ex. 1001, 10:56–11:3 (describing an administrator's finger press series mapping to a control signal to "[e]nroll an ordinary user"). The database is then populated "according to the instruction," as claimed, by storing the new user's master minutiae tables in memory. (Paper 1, 38-42; Ex. 1003, ¶¶ 231-245, pinpoint at ¶¶ 233-237).

Reply 23. Petitioner provides the following table which "summarizes how the prior art teaches Claims 1(d1)–1(d3)" (*id.*):

1(d1)-1(d3)	Petition's Mapping
Receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry	*Mathiassen's* processor receives information indicating a series of consecutive fingerprint representations i.e., a series of touches in a touch/no-touch sequence characterized according to the number of touches and duration of each touch (per *Anderson*).
Map said series into an instruction	*Mathiassen* translates the series of touches into a command using *Mathiassen's* command table.
Populate the data base according to the instruction	*Mathiassen+Anderson* renders obvious generating and storing master minutiae tables for a newly enrolled user according to the instruction to enroll commanded by the series of fingerprint representations in touch/no-touch sequence of particular durations.

Id. at 24.

Patent Owner argues that "Mathiassen has no teaching that either the 'predefined sets of finger movement sequences' or the 'command table' constitute a series of received biometric signal entries that are mapped into an instruction used to populate the database as part of the enrollment process." PO Resp. 33.

It is clear that Mathiassen's fingerprint sensor receives this series of entries of the biometric signal, similar to the '705 patent's code entry module 103 containing a biometric sensor 121 that receives a user's fingerprint. Ex. 1004 ¶ 192. Mathiassen's processor then translates the series of fingerprints received by its biometric sensor into a command, such as "open door" command, for authenticating the user to access the car doors. *Id*.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that the prior art discloses or suggests limitation 1(d3).

m) Clause 1(e)
"wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device"

Petitioner asserts "Mathiassen teaches the controlled item is a 'locking mechanism of a physical access structure' (i.e., the car door locks of the central locking system)." Pet. 42 (citing Ex. 1004 ¶ 187; Ex. 1003 ¶ 247 (testifying that Mathiassen discloses a controlled item that is a locking mechanism of a physical access structure, *i.e.* a car door). We also note that Mathiassen clearly discloses use of its disclosed computer-based locking and access system on a "laptop computer," "hotel safe," "medicine cabinet," and as a "door control" in "automotive applications." Ex. 1004 ¶¶ 41–44, 109–113.

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(e).

After having analyzed the entirety of the trial record and assigning appropriate weight to the cited supporting evidence, we determine Petitioner has shown by a preponderance of the evidence that, at the time of the filing of the '705 patent, one of ordinary skill would have been motivated to combine the teachings of Mathiassen, McKeeth, and Anderson in the manner recited in claim 1.

5. Analysis of Claims 4, 6, 10–12, and 14–17

Petitioner also provides an element-by-element analysis of where each element in the challenged claims 4, 6, 10–12, and 14–17 is disclosed in, or would have been obvious in view of, the cited references. Pet. 42–54. For clauses in claims 4, 6, 10–12, and 14–17 that are similar to those in claim 1, Petitioner refers to its arguments for claim 1, or other claims. *See, e.g.*, Pet. 49–50 (referring to its analysis for claim 14). Petitioner also provides a reason why it would have been obvious to modify and combine the references with a reasonable expectation of success, as proposed by Petitioner. *Id.* Petitioner also relies throughout the analysis of these claims on the testimony of Dr. Sears (Ex. 1003, 1090) for evidentiary support.

Patent Owner concedes that patentability of claims 4, 6, 10–12, and 14–17 stands or falls with patentability of independent claim 1. PO Resp. 35. Thus, applying the same analysis and evidence as discussed above in the context of claim 1, we determine that Petitioner has established by a preponderance of the evidence that dependent claims 4, 6, 10–12, and 14–17 of the '705 patent would have been obvious, and thus are not patentable.

III. CONCLUSION[24]

Petitioner has established by a preponderance of the evidence that claims 1, 4, 6, 10–12, and 14–17 are unpatentable.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, that Petitioner has shown by a preponderance of the evidence that claims 1, 4, 6, 10–12, and 14–17 are unpatentable.

V. SUMMARY TABLE

Claim(s)	35 U.S.C. §	Reference(s)/Basis	Claim(s) Shown Unpatentable	Claim(s) Not shown Unpatentable
1, 4, 6, 10–12, 14–17	103	Mathiassen, McKeeth, Anderson	1, 4, 6, 10–12, 14–17	
Overall Outcome			1, 4, 6, 10–12, 14–17	

[24] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

For PETITIONER:

Jennifer C. Bailey
Adam P. Seitz
ERISE IP, P.A.
jennifer.bailey@eriseip.com
adam.seitz@eriseip.com

For PATENT OWNER:

Darlene Ghavimi-Alagha
Brian Bozzo
K&L GATES LLP
darlene.ghavimi@klgates.com
brian.bozzo@klgates.com

US009269208B2

(12) **United States Patent**
Burke

(10) **Patent No.: US 9,269,208 B2**
(45) **Date of Patent: *Feb. 23, 2016**

(54) **REMOTE ENTRY SYSTEM**

(75) Inventor: **Christopher John Burke**, Ramsgate (AU)

(73) Assignee: **SECURICOM (NSW) PTY LTD**, Ramsgate (AU)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 78 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/572,166**

(22) Filed: **Aug. 10, 2012**

(65) **Prior Publication Data**

US 2012/0311343 A1 Dec. 6, 2012

Related U.S. Application Data

(63) Continuation of application No. 10/568,207, filed as application No. PCT/AU2004/001083 on Aug. 13, 2004, now Pat. No. 8,266,442.

(30) **Foreign Application Priority Data**

Aug. 13, 2003 (AU) 2003904317

(51) **Int. Cl.**
H04L 29/06 (2006.01)
G07C 9/00 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***G07C 9/00158*** (2013.01); ***G06F 21/32*** (2013.01); ***G06F 21/35*** (2013.01); ***H04L 63/0861*** (2013.01); ***H04W 12/08*** (2013.01); *H04W 84/12* (2013.01); *H04W 84/18* (2013.01)

(58) **Field of Classification Search**
CPC H04L 63/0861; G06F 21/32
USPC 713/186
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,109,428 A * 4/1992 Igaki et al. 382/125
5,933,515 A * 8/1999 Pu G06K 9/00006 340/5.53

(Continued)

FOREIGN PATENT DOCUMENTS

WO WO 0212660 A1 * 2/2002
WO WO 02/095589 A1 11/2002

OTHER PUBLICATIONS

Notice of Acceptance dated Sep. 18, 2012 for co-pending Australian Patent Office Application No. 2009201293 (3 pp.).

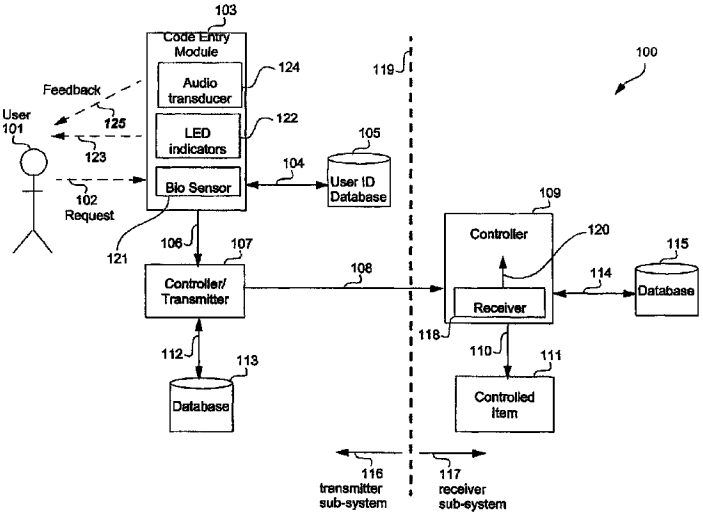
(Continued)

Primary Examiner — Mohammad L Rahman
(74) *Attorney, Agent, or Firm* — Brinks Gilson & Lione

(57) **ABSTRACT**

A system is disclosed for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol, and a receiver sub-system comprising means for receiving the transmitted secure access signal and means for providing conditional access to the controlled item dependent upon said information.

13 Claims, 10 Drawing Sheets



(51) **Int. Cl.**

G06F 21/32	(2013.01)
G06F 21/35	(2013.01)
H04W 12/08	(2009.01)
H04W 84/12	(2009.01)
H04W 84/18	(2009.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,195,447	B1 *	2/2001	Ross	382/125
6,229,906	B1 *	5/2001	Pu et al.	382/116
6,992,562	B2 *	1/2006	Fuks et al.	340/5.52
7,152,045	B2 *	12/2006	Hoffman	705/43
7,174,017	B2 *	2/2007	Bantz et al.	380/255
2002/0038818	A1	4/2002	Zingher et al.	
2003/0126439	A1	7/2003	Wheeler et al.	
2004/0042642	A1 *	3/2004	Bolle	G07C 9/00134 382/115

OTHER PUBLICATIONS

Extended European Search Report for corresponding EP application No. 14188004 dated Apr. 22, 2015.
Office Action for corresponding Canadian application No. 2,535,434 dated Mar. 27, 2015.

* cited by examiner

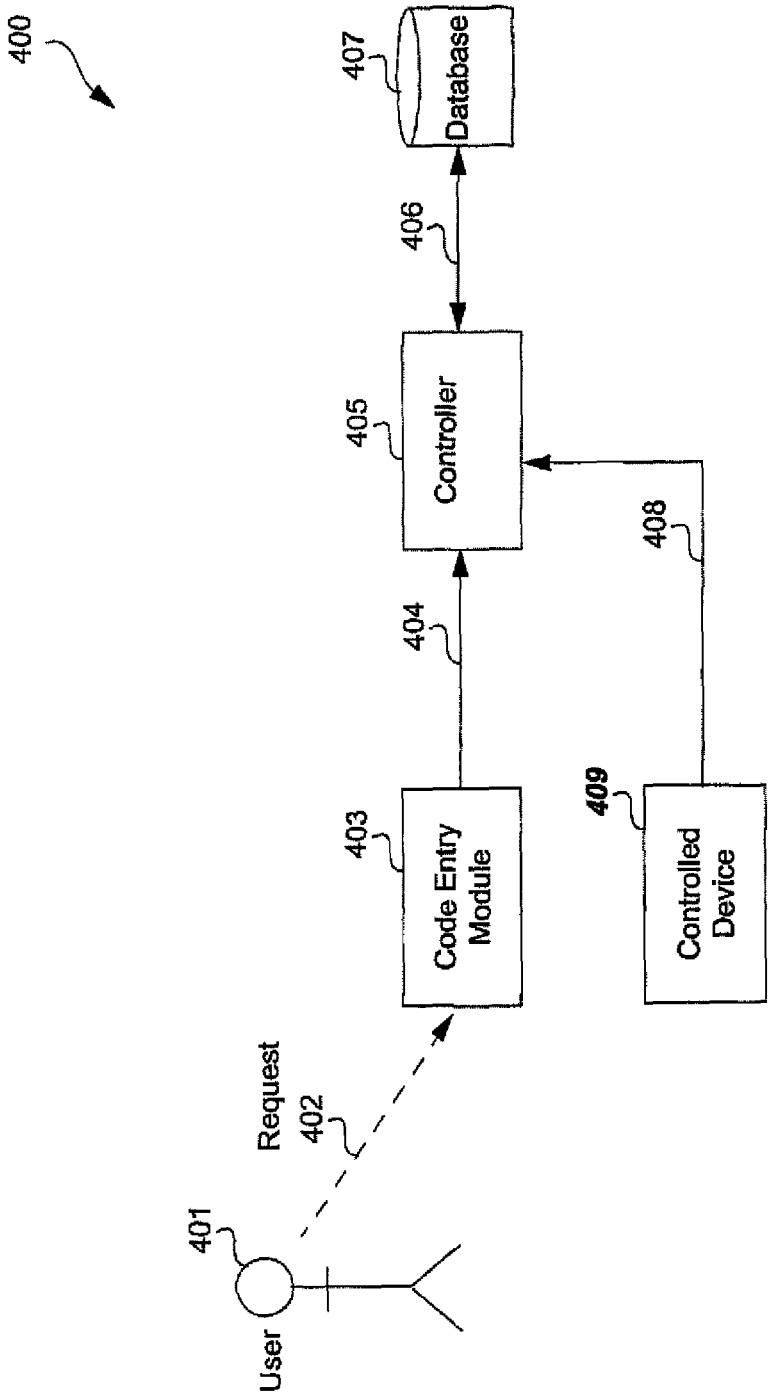


Fig. 1
(prior art)

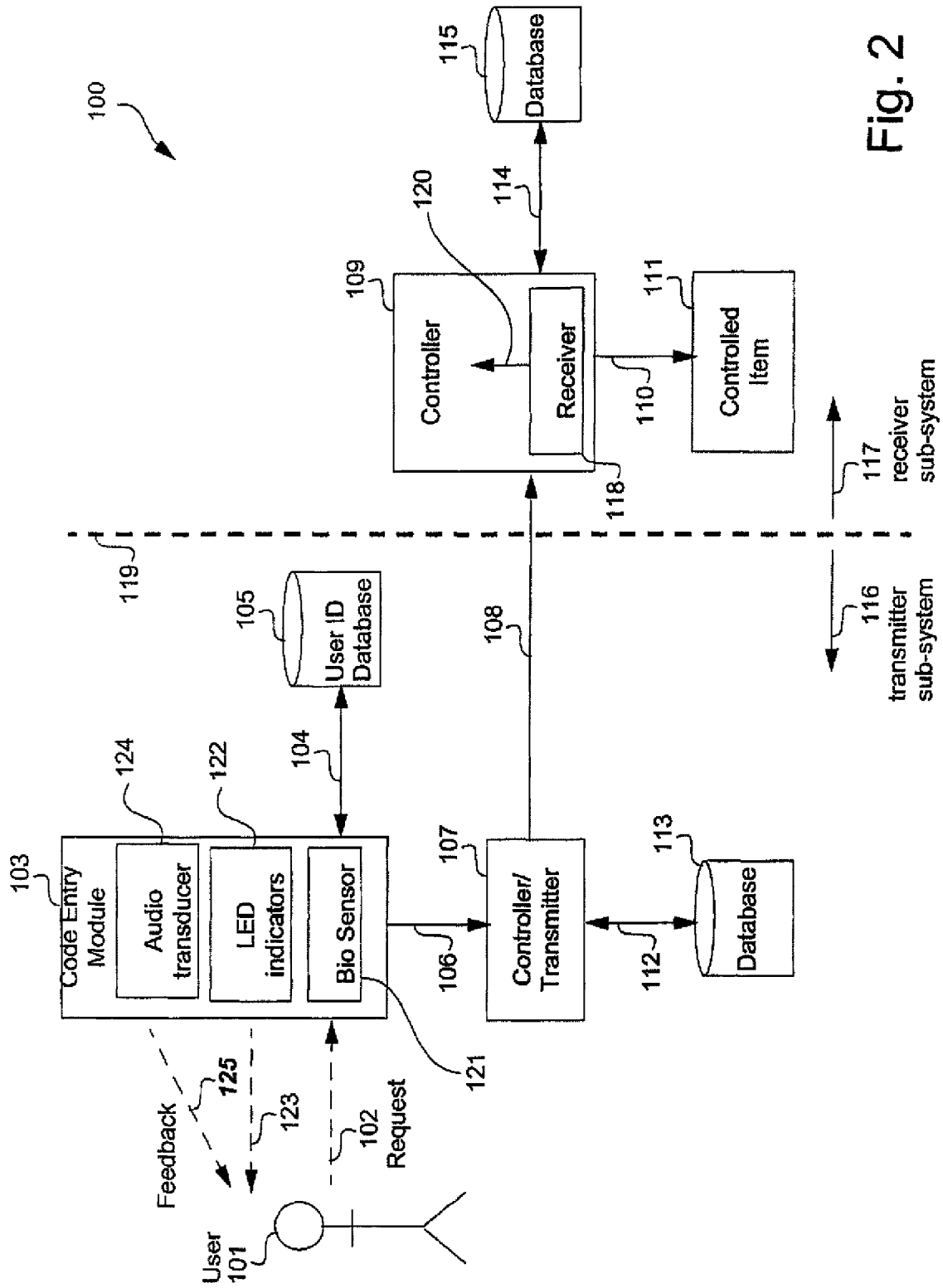


Fig. 2

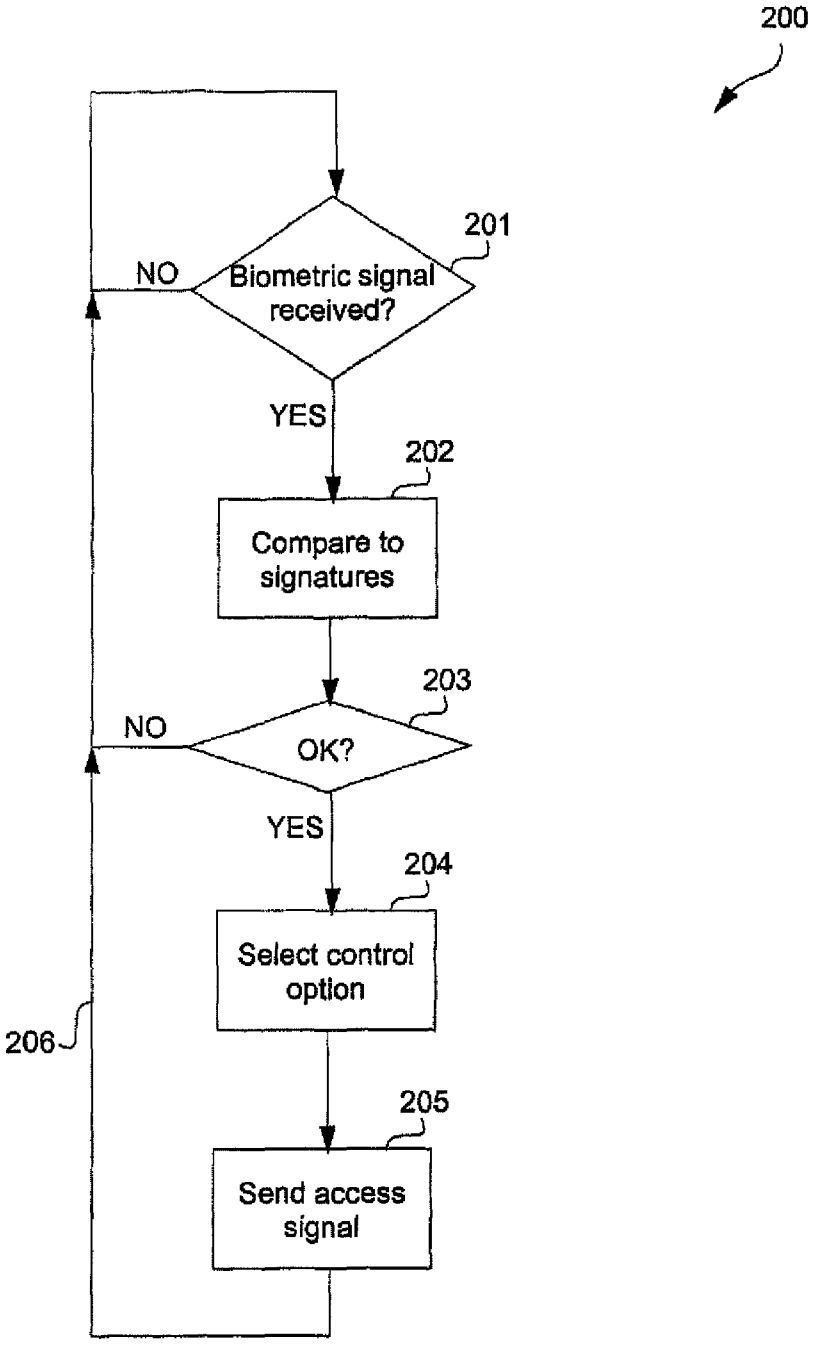

200
201
Biometric signal received?
NO
YES
202
Compare to signatures
203
OK?
NO
YES
204
Select control option
205
Send access signal
206

Fig. 3

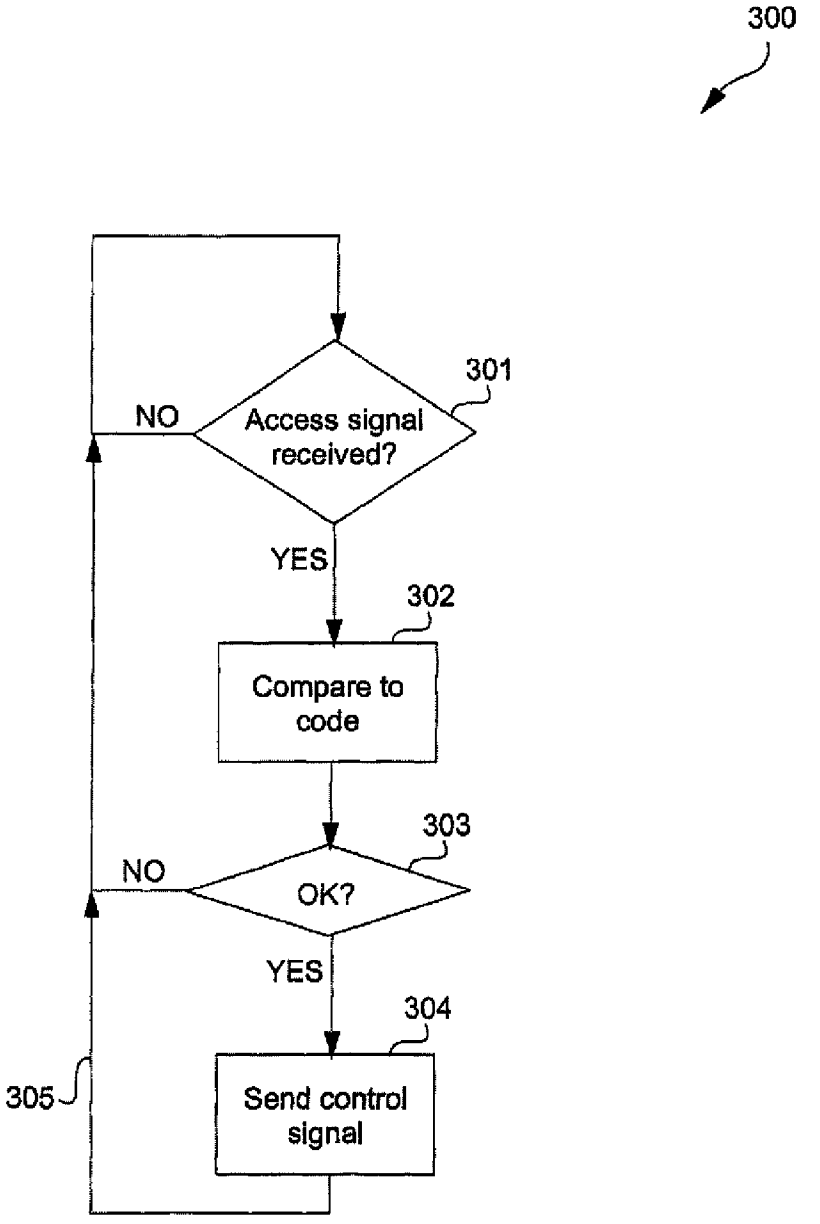

300
301
Access signal received?
NO
YES
302
Compare to code
303
OK?
NO
YES
304
Send control signal
305

Fig. 4

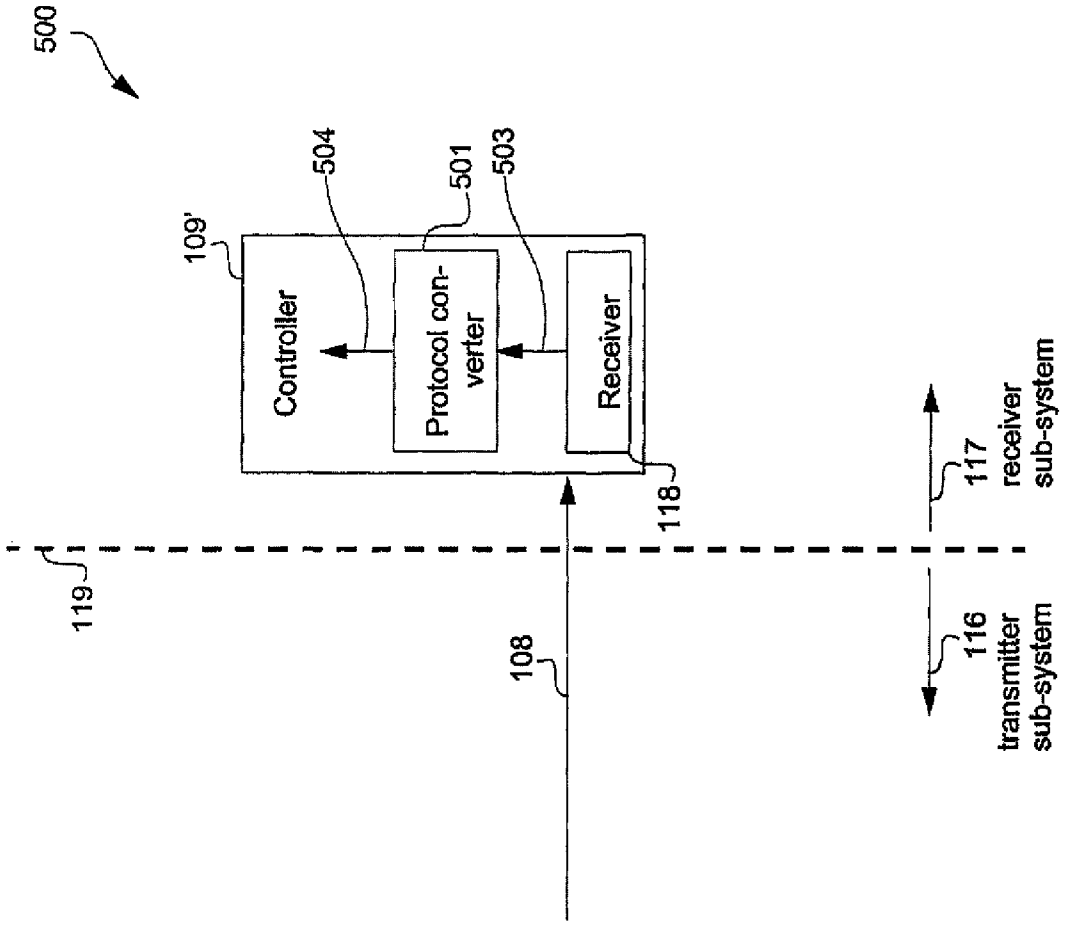

500
504
501
503
109'
Controller
Protocol con-
verter
Receiver
118
119
108
117
receiver
sub-system
116
transmitter
sub-system

Fig. 5

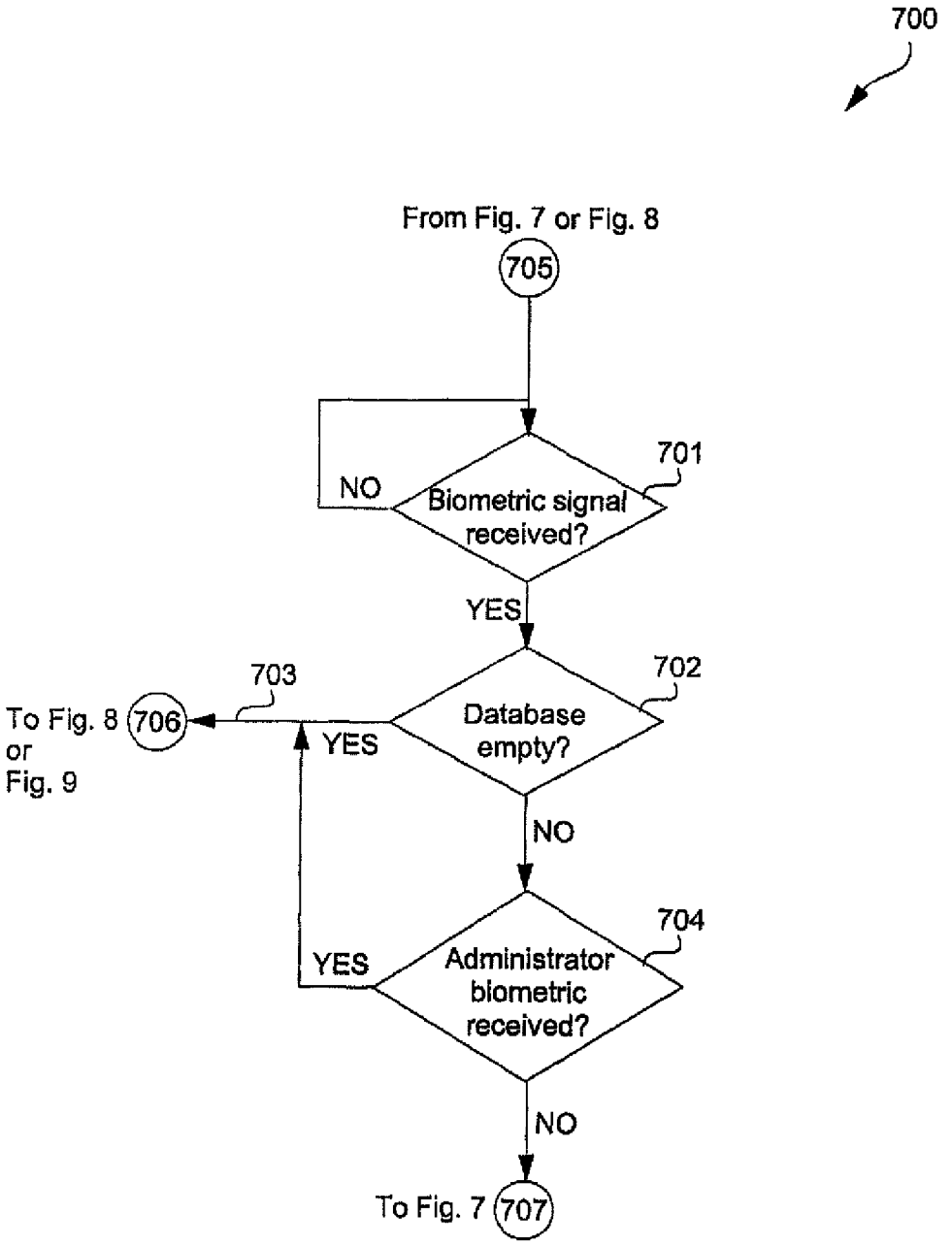

700
From Fig. 7 or Fig. 8
705
701
NO
Biometric signal received?
YES
703
702
To Fig. 8 706
or
Fig. 9
YES
Database empty?
NO
704
YES
Administrator biometric received?
NO
To Fig. 7 707

Fig. 6

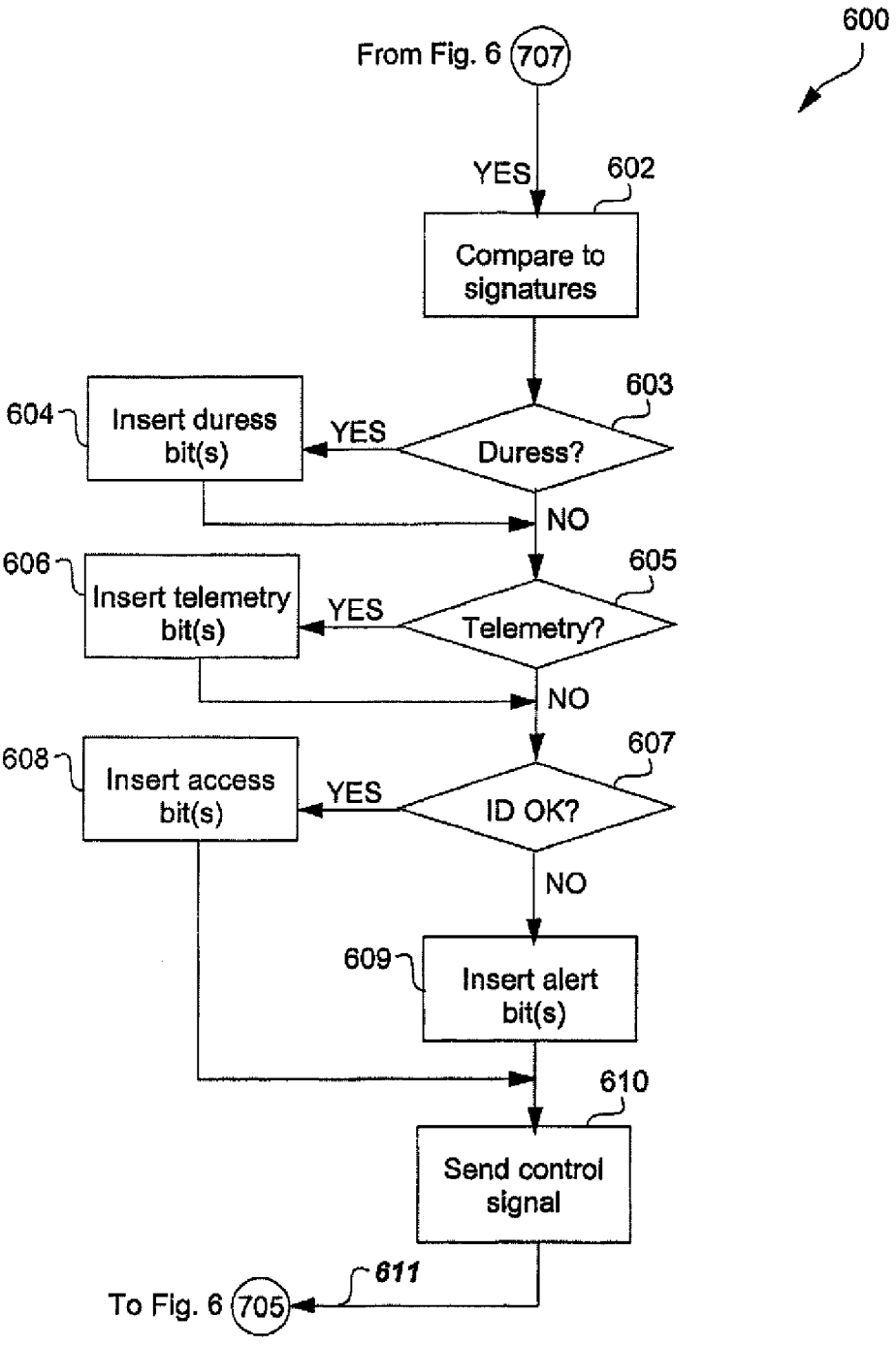

600
From Fig. 6
707
YES
602
Compare to signatures
603
604
Insert duress bit(s)
YES
Duress?
NO
606
Insert telemetry bit(s)
YES
605
Telemetry?
NO
608
Insert access bit(s)
YES
607
ID OK?
NO
609
Insert alert bit(s)
610
Send control signal
611
To Fig. 6
705

Fig. 7

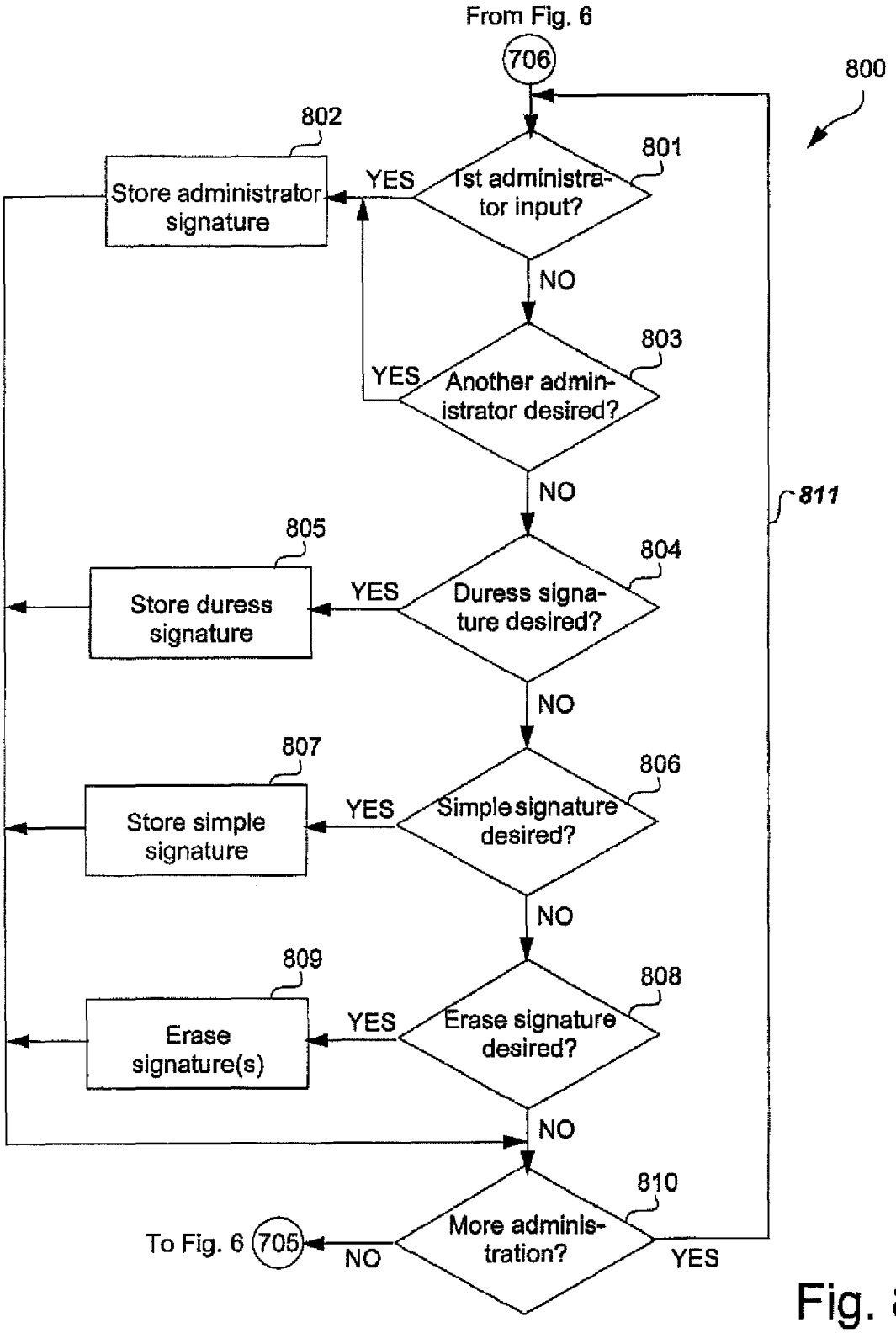

From Fig. 6
706
800
802
801
Store administrator signature
YES
1st administrator input?
NO
803
YES
Another administrator desired?
NO
811
805
804
Store duress signature
YES
Duress signature desired?
NO
807
806
Store simple signature
YES
Simple signature desired?
NO
809
808
Erase signature(s)
YES
Erase signature desired?
NO
810
To Fig. 6
705
NO
More administration?
YES

Fig. 8

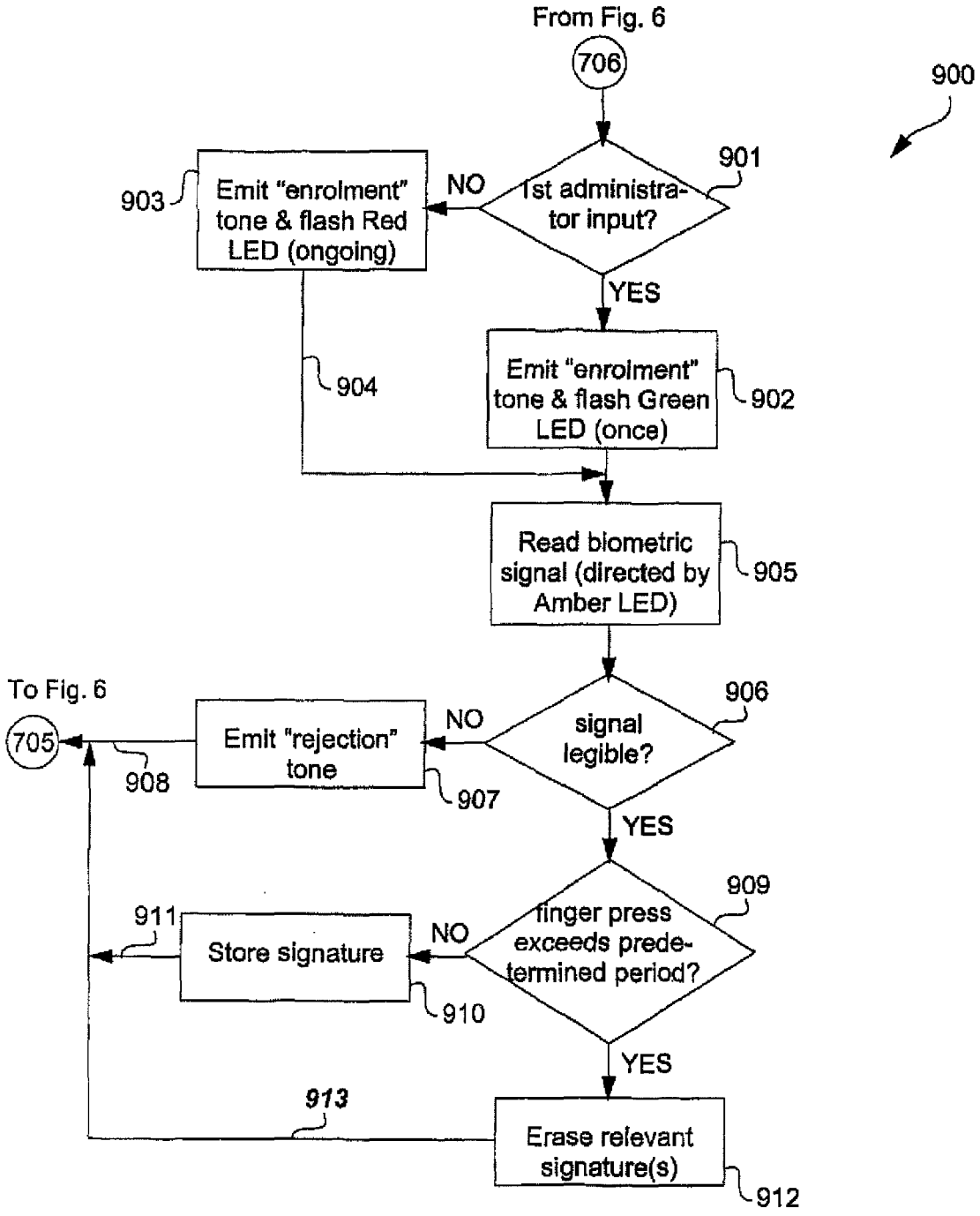

From Fig. 6
706
900
901
1st administrator input?
NO
YES
903
Emit "enrolment" tone & flash Red LED (ongoing)
904
Emit "enrolment" tone & flash Green LED (once)
902
Read biometric signal (directed by Amber LED)
905
To Fig. 6
705
906
signal legible?
NO
908
Emit "rejection" tone
907
YES
909
finger press exceeds predetermined period?
911
Store signature
NO
910
YES
913
Erase relevant signature(s)
912

Fig. 9

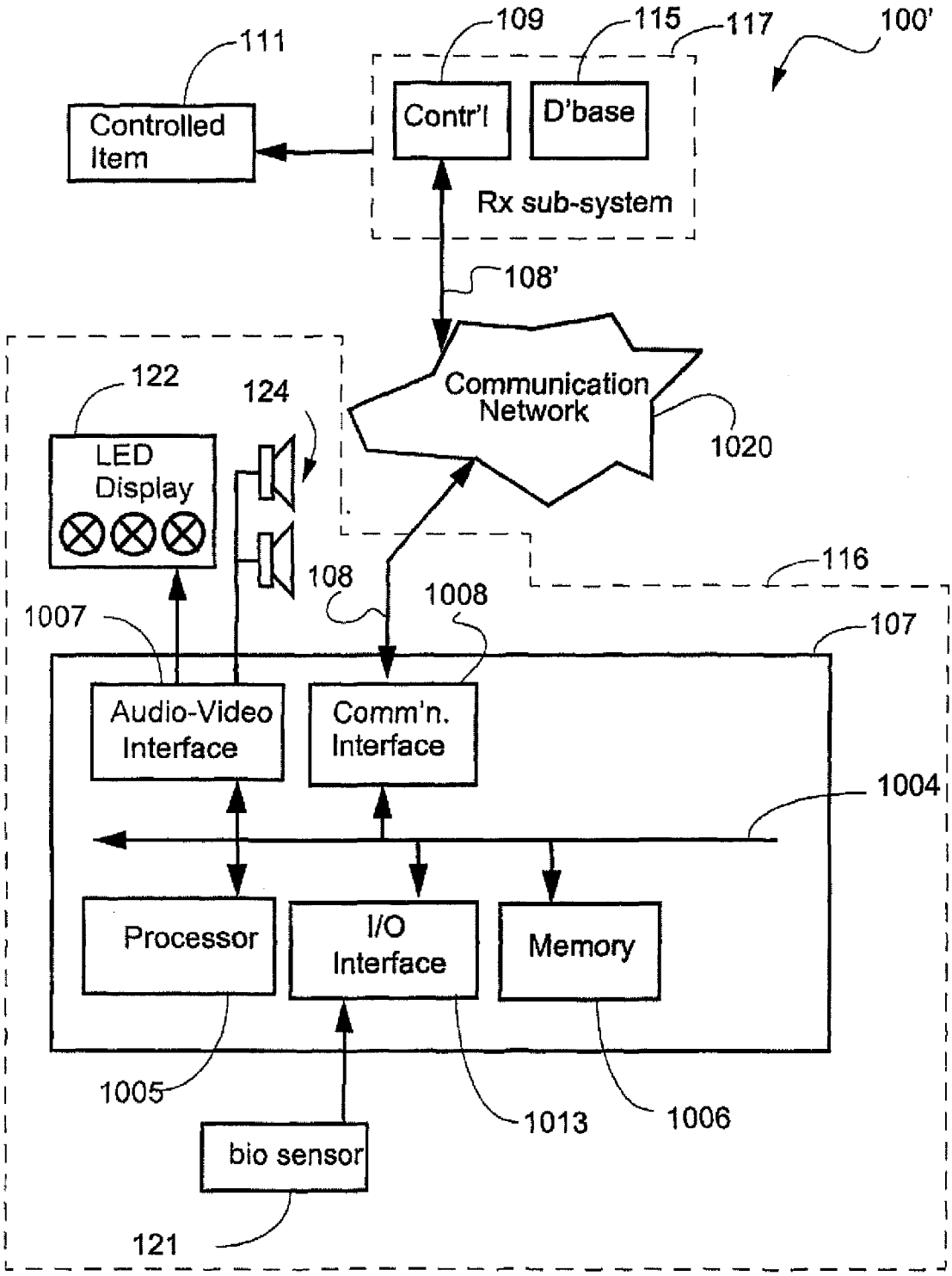

111
109
115
117
100'
Controlled Item
Contr'l
D'base
Rx sub-system
108'
Communication Network
1020
122
124
LED Display
108
116
1008
1007
107
Audio-Video Interface
Comm'n. Interface
1004
Processor
I/O Interface
Memory
1005
1013
1006
bio sensor
121

Fig. 10

REMOTE ENTRY SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation patent application of U.S. Non-Provisional application Ser. No. 10/568,207 for REMOTE ENTRY SYSTEM, filed Jun. 4, 2008 now U.S. Pat. No. 8,266,442, the disclosure of which is incorporated by reference in its entirety.

FIELD OF THE INVENTION

The present invention relates to secure access systems and, in particular, to systems using wireless transmission of security code information.

BACKGROUND

FIG. **1** shows a prior art arrangement for providing secure access. A user **401** makes a request, as depicted by an arrow **402**, directed to a code entry module **403**. The module **403** is typically mounted on the external jamb of a secure door. The request **402** is typically a secure code of some type which is compatible with the code entry module **403**. Thus, for example, the request **402** can be a sequence of secret numbers directed to a keypad **403**. Alternately, the request **402** can be a biometric signal from the user **401** directed to a corresponding biometric sensor **403**. One example of a biometric signal is a fingerprint. Other physical attributes that can be used to provide biometric signals include voice, retinal or iris pattern, face pattern, palm configuration and so on.

The code entry module **403** conveys the request **402** by sending a corresponding signal, as depicted by an arrow **404**, to a controller **405** which is typically situated in a remote or inaccessible place. The controller **405** authenticates the security information provided by the user **401** by interrogating a database **407** as depicted by an arrow **406**. If the user **401** is authenticated, and has the appropriate access privileges, then the controller **405** sends an access signal, as depicted by an arrow **408**, to a device **409** in order to provide the desired access. The device **409** can, for example, be the locking mechanism of a secure door, or can be an electronic lock on a personal computer (PC) which the user **401** desires to access.

A proximity card can also be used to emit the request **402**, in which case the code entry module **403** has appropriate functionality.

Although the request **402** can be made secure, either by increasing the number of secret digits or by using a biometric system, the communication infrastructure in FIG. **1** is typically less secure. The infrastructure **400** is generally hardwired, with the code entry module **403** generally being mounted on the outside jamb of a secured door. In such a situation, the signal path **404** can be over a significant distance in order to reach the controller **405**. The path **404** represents one weak point in the security system **400**, providing an unauthorised person with relatively easy access to the information being transmitted between the code entry module **403** and the controller **405**. Such an unauthorised person can, given this physical access, decipher the communicated information between the code entry module **403** and the controller **405**. This captured information can be deciphered, replayed in order to gain the access which rightfully belongs to the user **401**, or to enable modification for other subversive purposes.

Current systems as depicted in FIG. **1** utilise a communication protocol called "Wiegand" for communication between the code entry module **403** and the controller **405**.

The Wiegand protocol is a simple one-way data protocol that can be modified by increasing or decreasing the bit count to ensure uniqueness of the protocol among different security companies. The Wiegand protocol does not secure the information being sent between the code entry module **403** and the controller **405**.

More advanced protocols such as RS **485** have been used in order to overcome the vulnerability of the Wiegand protocol over the long distance route **404**. RS **485** is a duplex protocol offering encryption capabilities at both the transmitting and receiving ends, i.e. the code entry module **403** and the controller **405** respectively in the present case. The length of the path **404** nonetheless provides an attack point for the unauthorised person.

Due to the cost and complexity of re-wiring buildings and facilities, security companies often make use of existing communication cabling when installing and/or upgraded security systems, thereby maintaining the vulnerability described above.

SUMMARY

It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

According to a first aspect of the present invention, there is provided a system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a transmitter subsystem comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; and a receiver sub-system comprising;

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a transmitter sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a receiver sub-system comprising means for receiving a secure access signal transmitted by the transmitter sub-system, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal; wherein the transmitter subsystem comprises:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

means for emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol.

According to another aspect of the present invention, there is provided receiver sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against

members of the database of biometric signatures to thereby output an accessibility attribute, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; wherein the receiver sub-system comprises;

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a method for providing secure access to a controlled item, the method comprising the steps of:

receiving a biometric signal;

matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute;

emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; and

providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a method for populating a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon information in said secure access signal, said method comprising the steps of:

receiving a series of entries of the biometric signal;

determining at least one of the number of said entries and a duration of each said entry;

mapping said series into an instruction; and

populating the database according to the instruction.

According to another aspect of the present invention, there is provided a method for transmitting a secure access signal in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a receiver sub-system comprising means for receiving the secure access signal transmitted by a transmitter sub-system, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal, said method comprising the steps of:

receiving a biometric sensor by biometric signal;

matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol.

According to another aspect of the present invention, there is provided a method for receiving a secure access signal in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol, said method comprising the steps of:

receiving the transmitted secure access signal; and

providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to provide secure access to a controlled item, said computer program product comprising:

code for receiving a biometric signal;

code for matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute;

code for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; and

code for providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to populate a database of biometric signatures in a system for providing secure access to a controlled item, said computer program product comprising:

code for receiving a series of entries of the biometric signal;

code for determining at least one of the number of said entries and a duration of each said entry;

code for mapping said series into an instruction; and

code for populating the database according to the instruction.

According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to transmit a secure access signal in a system for providing secure access to a controlled item, said computer program product comprising:

code for receiving a biometric sensor by biometric signal;

code for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

code for emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol.

According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to receive a secure access signal in a system for providing secure access to a controlled item, said computer program product comprising:

code for receiving the transmitted secure access signal; and

code for providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a system for providing secure access, the system comprising:

a biometric sensor for authenticating the identity of a user;

a transmitter for transmitting information using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and

a control panel for receiving the information and for providing the secure access requested.

Other aspects of the invention are also disclosed.

BRIEF DESCRIPTION OF THE DRAWINGS

Some aspects of the prior art and one or more embodiments of the present invention are described with reference to the drawings, in which:

FIG. **1** shows a prior art arrangement for providing secure access;

FIG. **2** is a functional block diagram of an arrangement for providing secure access according to the present disclosure;

FIG. **3** shows an example of a method of operation of the remote control module of FIG. **2**;

FIG. **4** shows an example of a method of operation of the (fixed) control device of FIG. **2**;

FIG. **5** shows incorporation of a protocol converter into the arrangement of FIG. **2**; and

FIG. **6** shows another example of how the remote access system operates;

FIG. **7** shows an access process relating to the example of FIG. **6**;

FIG. **8** shows one enrolment process relating to the example of FIG. **6**;

FIG. **9** shows another enrolment process relating to the example of FIG. **6**; and

FIG. **10** is a schematic block diagram of the system in FIG. **2**.

DETAILED DESCRIPTION INCLUDING BEST MODE

It is to be noted that the discussions contained in the "Background" section relating to prior art arrangements relate to discussions of documents or devices which form public knowledge through their respective publication and/or use. Such should not be interpreted as a representation by the present inventor(s) or patent applicant that such documents or devices in any way form part of the common general knowledge in the art.

Where reference is made in any one or more of the accompanying drawings to steps and/or features, which have the same reference numerals, those steps and/or features have for the purposes of this description the same function(s) or operation(s), unless the contrary intention appears.

FIG. **2** is a functional block diagram of an arrangement for providing secure access according to the present disclosure. A user **101** makes a request, as depicted by an arrow **102**, to a code entry module **103**. The code entry module **103** includes a biometric sensor **121** and the request **102** takes a form which corresponds to the nature of the sensor **121** in the module **103**. Thus, for example, if the biometric sensor **121** in the code entry module **103** is a fingerprint sensor, then the request **102** typically takes the form of a thumb press on a sensor panel (not shown) on the code entry module **103**.

The code entry module **103** interrogates, as depicted by an arrow **104**, a user identity database **105**. Thus for example if the request **102** is the thumb press on the biometric sensor panel **121** then the user database **105** contains biometric signatures for authorised users against which the request **102** can be authenticated. If the identity of the user **101** is authenticated successfully, then the code entry module **103** sends a signal **106** to a controller/transmitter **107**. The controller/transmitter **107** checks, as depicted by an arrow **112**, the current rolling code in a database **113**. The controller **107** then updates the code and sends the updated code, this being referred to as an access signal, as depicted by an arrow **108** to a controller **109**. The rolling code protocol offers non-replay encrypted communication.

The controller **109** tests the rolling code received in the access signal **108** against the most recent rolling code which has been stored in a database **115**, this testing being depicted by an arrow **114**. If the incoming rolling code forming the access signal **108** is found to be legitimate, then the controller **109** sends a command, as depicted by an arrow **110**, to a controlled item **111**. The controlled item **111** can be a door locking mechanism on a secure door, or an electronic key circuit in a personal computer (PC) that is to be accessed by the user **101**. It is noted that the controller **109** contains a receiver **118** that receives the transmitted access signal **108** and converts it into a form that is provided, as depicted by an arrow **120**, into a form that the controller **109** can use.

The code entry module **103** also incorporates at least one mechanism for providing feedback to the user **101**. This mechanism can, for example, take the form or one or more Light Emitting Diodes (LEDs) **122** which can provide visual feedback, depicted by an arrow **123** to the user **101**. Alternately or in addition the mechanism can take the form of an audio signal provided by an audio transducer **124** providing audio feedback **125**.

The arrangement in FIG. **2** has been described for the case in which the secure code in the access signal **108** used between the sub-systems **116** and **117** is based upon the rolling code. It is noted that this is merely one arrangement, and other secure codes can equally be used. Thus, for example, either of the Bluetooth™ protocol, or the Wi Fi™ protocols can be used.

Rolling codes provide a substantially non-replayable non-repeatable and encrypted radio frequency data communications scheme for secure messaging. These codes use inherently secure protocols and serial number ciphering techniques which in the present disclosure hide the clear text values required for authentication between the key fob (transmitter) sub-system **116** and the receiver/controller **118**/**109**.

Rolling codes use a different code variant each time the transmission of the access signal **108** occurs. This is achieved by encrypting the data from the controller **107** with a mathematical algorithm, and ensuring that successive transmissions of the access signal **108** are modified using a code and/or a look-up table known to both the transmitter sub-system **116** and the receiver sub-system **117**. Using this approach successive transmissions are modified, resulting in a non-repeatable data transfer, even if the information from the controller **107** remains the same. The modification of the code in the access signal **108** for each transmission significantly reduces the likelihood that an intruder can access the information replay the information to thereby gain entry at some later time.

The sub-system in FIG. **2** falling to the left hand side, as depicted by an arrow **116**, of a dashed line **119** can be implemented in a number of different forms. The sub-system **116** can for example be incorporated into a remote fob (which is a small portable device carried by the user **101**), or alternately can be mounted in a protected enclosure on the outside jamb of a secured door. The sub-system **116** communicates with the sub-system **117** on the right hand side of the dashed line **119** via the wireless communication channel used by the access signal **108**. The sub-system **117** is typically located in an inaccessible area such as a hidden roof space or alternately in a suitable protected area such as an armoured cupboard.

The location of the sub-system **117** must of course be consistent with reliable reception of the wireless access signal **108**.

Although typically the communication channel uses a wireless transmission medium, there are instances where the channel used by the access signal **108** can use a wired medium. This is particularly the case when the transmitter sub-system **116** is mounted in an enclosure on the door jamb rather than in a portable key fob.

The biometric signature database **105** is shown in FIG. **2** to be part of the transmitter sub-system **116**. However, in an alternate arrangement, the biometric signature database **105** can be located in the receiver sub-system **117**, in which case the communication **104** between the code entry module **103** and the signature database **105** can also be performed over a secure wireless communication channel such as the one used by the access signal **108**. In the event that the secure access system is being applied to providing secure access to a PC, then the secured PC can store the biometric signature of the authorised user in internal memory, and the PC can be integrated into the receiver sub-system **117** of FIG. **1**.

In the event that the sub-system **116** is implemented as a remote fob, the combination of the biometric verification and the strongly encrypted wireless communication provides a particularly significant advantage over current systems. The remote key fob arrangement allows easy installation, since the wired communication path **404** (see FIG. **1**) is avoided. Other existing wiring elements of the present systems **400** can be used where appropriate. When the sub-system **116** is implemented as a remote fob, the fob incorporates the biometric (eg fingerprint) authentication arrangement, in which case only one biometric signature is stored in the fob. This arrangement reduces the requirements on the central database **115**. Once the key fob authenticates the user through biometric signature (eg fingerprint) verification, the rolling code in the access signal **108** is transmitted to the controller **109** for authorisation of the user for that location at that time.

In addition to authenticating the user **101** the biometric sensor **121** in the code entry module **103** in conjunction with the controller **107** can also check other access privileges of the user **101**. These access privileges can be contained in the database **105** which can be located either locally in the remote key fob, or in the receiver sub-system **117** as previously described. In one example, Tom Smith can firstly be authenticated as Tom Smith using the thumb press by Tom on the biometric sensor panel (not shown). After Tom's personal biometric identity is authenticated, the transmitter sub-system **116** can check if Tom Smith is in fact allowed to use the particular door secured by the device **111** on weekends. Thus the security screening offered by the described arrangement can range from simple authentication of the user's identity, to more comprehensive access privilege screening.

The incorporation of the biometric sensor **121** into the code entry module **103** in the form of a remote key fob also means that if the user **101** loses the remote key fob, the user need not be concerned that someone else can use it. Since the finder of the lost key fob will not be able to have his or her biometric signal authenticated by the biometric sensor **121** in the code entry module **103**, the lost key fob is useless to anyone apart from the rightful user **101**.

The transmitter sub-system **116** is preferably fabricated in the form of a single integrated circuit (IC) to reduce the possibility of an authorised person bypassing the biometric sensor **121** in the code entry module **103** and directly forcing the controller **107** to emit the rolling code access signal **108**.

FIG. **3** shows the method of operation of the remote control module (i.e. the sub-system **116**) of FIG. **2**. The method **200** commences with a testing step **201** in which the biometric sensor **121** in the code entry module **103** checks whether a biometric signal **102** is being received. If this is not the case, then the method **200** is directed in accordance with an NO arrow back to the step **201** in a loop. If, on the other hand, the biometric signal **102** has been received, then the method **200** is directed in accordance with a YES arrow to a step **202**. The step **202** compares the received biometric signal **102** with information in the biometric signature database **105** in order to ensure that the biometric signal received **102** is that of the rightful user **101** of the sub-system **116**.

A subsequent testing step **203** checks whether the comparison in the step **202** yields the desired authentication. If the biometric signature matching is authenticated, then the process **200** is directed in accordance with a YES arrow to a step **204**. The authentication of the biometric signature matching produces an accessibility attribute for the biometric signal **102** in question. The accessibility attribute establishes whether and under which conditions access to the controlled item **111** should be granted to a user. Thus, for example, the accessibility attribute may comprise one or more of an access attribute (granting unconditional access), a duress attribute (granting access but with activation of an alert tone to advise authorities of the duress situation), an alert attribute (sounding a chime indicating that an unauthorised, but not necessarily hostile, person is seeking access, and a telemetry attribute, which represents a communication channel for communicating state information for the transmitter sub-system to the receiver sub-system such as a "low battery" condition. The step **204** enables the user **101** to select a control option by providing one or more additional signals (not shown) to the controller **107**. Thus for example the control option could enable the user **101** to access one of a number of secure doors after his or her identity has been authenticated in the step **203**. In the subsequent step **205** the controller **107** sends the appropriate access signal **108** to the controller **109**. The process **200** is then directed in accordance with an arrow **206** back to the step **201**.

Thus for example the sub-system **116** can be provided with a single biometric sensor **121** in the code entry module **103** which enables the user **101** to select one of four door entry control signals by means of separate buttons on the controller **107** (not shown). This would enable the user **101**, after authentication by the biometric sensor **121** in the code entry module **103** and the controller **107** to obtain access to any one of the aforementioned for secure doors.

Returning to the testing step **203**, if the signature comparison indicates that the biometric signal **102** is not authentic, and has thus not been received from the proper user, then the process **200** is directed in accordance with a NO arrow back to the step **201**. In an alternate arrangement, the NO arrow from the step **203** could lead to a disabling step which would disable further operation of the sub-system **116**, either immediately upon receipt of the incorrect biometric signal **102**, or after a number of attempts to provide the correct biometric signal **102**.

FIG. **4** shows the method of operation of the control subsystem **117** of FIG. **2**. The method **300** commences with a testing step **301** which continuously checks whether the access signal **108** has been received from **107**. The step **301** is performed by the controller **109**. As long as the access signal **108** is not received the process **300** is directed in accordance with a NO arrow in a looping manner back to the step **301**. When the access signal **108** is received, the process **300** is directed from the step **301** by means of a YES arrow to a step **302**. In the step **302**, the controller **109** compares the rolling code received by means of the access signal **108** with a reference code in the database **115**. A subsequent testing step

303 is performed by the controller 109. In the step 303 if the code received on the access signal 108 is successfully matched against the reference code in the database 115 then the process 300 is directed in accordance with a YES arrow to a step 304.

In the step 304 the controller 109 sends the control signal 110 to the controlled item 111 (for example opening the secured door). The process 300 is then directed from the step 304 as depicted by an arrow 305 back to the step 301. Returning to the testing step 303 if the code received on the access signal 108 is not successfully matched against the reference code in the database 115 by the controller 109 then the process 300 is directed from the step 303 in accordance with a NO arrow back to the step 301.

As was described in regard to FIG. 3, in an alternate arrangement, the process 300 could be directed, if the code match is negative, from the step 303 to a disabling step which would disable the sub-system 117 if the incorrect code where received once or a number of times.

FIG. 5 shows incorporation of a protocol converter into the arrangement of FIG. 2. In the arrangement of FIG. 2 the receiver 118 in the controller 109 is able to directly receive and process the rolling code in the access signal 108 in a manner as to provide, as depicted by the arrow 120, the necessary information to the controller 109. FIG. 5 shows how an existing controller depicted by a reference numeral 109' that uses Wiegand input signalling can be used in the disclosed arrangement when alarm systems are upgraded. FIG. 5 shows how the incoming access signal 108 is received by a receiver 118' as is the case in FIG. 2. In FIG. 5 however the receiver 118' provides, as depicted by an arrow 503, the received rolling code from the access signal 108 to a rolling code/Wiegand protocol converter 501. The converter 501 converts, as depicted by an arrow 504, the incoming rolling code 503 to a form that can be used by the controller 109' that is designed to handle Wiegand protocol incoming signals. Therefore, the converted incoming signal 504 is in the Wiegand format.

The converter 501 uses a microprocessor-based arrangement running software code to process the incoming rolling code information 503 and decode this information 503 to clear text form. The converter 501 converts this clear text to a Wiegand variable bit-length data stream. In FIG. 2, the receiver 118 performs the conversion of the incoming rolling code access signal 108 to clear text which enables the controller 109 to identify the serial number of the originating key fob sub-system 116 to enable the access rights of the user to be verified.

Further to the Wiegand conversion arrangement, the protocol converter 501 approach can be adapted to convert between the incoming rolling code 503 (or any other appropriate secure code) to any other convenient protocol used by the controller 169'

The advantage of the rolling code/Wiegand converter 501 is that security system upgrades can be made without replacing Wiegand compatible controller 109'. Accordingly, existing systems as are described in FIG. 1 can be upgraded by replacing the code entry module 403 and the transmission path 404, leaving the other components of the system 400 (i.e., the controller 405, the code database 407, and the controlled item 409, together with existing wiring 408 and 406), largely intact. Minor modifications might however be necessary. When upgrading systems in this manner, the sub-system 116 can either be used in a remote fob configuration, or can be placed in a secure housing on an external door jamb.

From a practical perspective, incorporating the protocol converter 501 into an existing controller 109' would require direct wiring of the converter 501 into the housing of the secure controller 109'.

FIG. 6 shows another process 700 of operation of the remote access system. The process 700 commences with a step 701 that determines if a biometric signal has been received by the biometric sensor 121 in the code entry module in FIG. 2. If not, then the process 700 follows a NO arrow back to the step 701. If however a biometric signal has been received, then the process 700 follows a YES arrow to a step 702 that determines if the user ID database 105 in FIG. 2 is empty. This would be the case, for example, if the code entry module is new and has never been used, or if the user 101 has erased all the information in the database 105.

If the database 105 is empty, then the process 700 is directed by an arrow 703 to 706 in FIG. 8 which depicts a process 800 dealing with the enrolment or the administration function for loading relevant signatures into the database 105. If on the other hand the database 105 is not empty, then the process 700 is directed to a step 704 that determines if the biometric signal that has been received is an administrator's biometric signal.

The disclosed remote entry system can accommodate at least three classes of user, namely administrators, (ordinary) users, and duress users. The administrators have the ability to amend data stored, for example, in the database 105, while the ordinary users do not have this capability. The first user of the code entry module 103, whether this is the user who purchases the module, or the user who programs the module 103 after all data has been erased from the database 105, is automatically categorised as an administrator. This first administrator can direct the system 100 to either accept further administrators, or alternately to only accept further ordinary users.

Although the present description refers to "Users", in fact it is "fingers" which are the operative entities in system operation when the biometric sensor 121 (see FIG. 2) is a fingerprint sensor. In this event, a single user can enrol two or more of his or her own fingers as separate administrators or (ordinary) users of the system, by storing corresponding fingerprints for corresponding fingers in the database 105 via the enrolment process 800 (see FIG. 8).

Some class overlap is possible. Thus a stored signature can belong to an administrator in the duress class.

The first administrator can provide control information to the code entry module by providing a succession of finger presses to the biometric sensor 121, providing that these successive presses are of the appropriate duration, the appropriate quantity, and are input within a predetermined time. In one arrangement, the control information is encoded by either or both (a) the number of finger presses and (b) the relative duration of the finger presses. If the successive finger presses are provided within this predetermined time, then the controller 107 accepts the presses as potential control information and checks the input information against a stored set of legal control signals.

One example of a legal control signal can be expressed as follows:

"Enrol an ordinary user"→dit, dit, dit, dah

where "dit" is a finger press of one second's duration (provided by the user 101 in response to the feedback provided by the Amber LED as described below), and "dah" is a finger press of two second's duration.

In the event that a legitimate sequence of finger presses are not delivered within the predetermined time, then the presses are considered not to be control information and merely to be presses intended to provide access to the controlled item 111.

Legitimate control sequences are defined in Read Only Memory (ROM) in the controller **107**.

The code entry module **103** has feedback signalling mechanisms **122**, implemented for example by a number of LEDs, and **124**, implemented by an audio transducer. The LEDs **122** and the audio transducer **124** are used by the controller to signal the state of the code entry module **103** to the user **101**, and to direct the administration process. Thus, in one example, three LEDs, being Red, Amber and Green are provided.

When the Amber LED is flashing, it means "Press the sensor". When the Amber LED is steady ON, it means "Maintain finger pressure". When the Amber LED is OFF, it means "Remove finger pressure". When the system enters the enrolment state (depicted by the process **800** in FIG. **8**), then the audio transducer **124** emits the "begin enrolment" signal (dit dit dit dit) and the Red LED flashes. Enrolment of a normal user (according to the step **807** in FIG. **8**) is signalled by the OK audio signal (dit dit) and a single blink of the Green LED.

Returning to the step **704**, if the step determines that the biometric signal received is an administrator's signal, then the process **700** is directed by a YES arrow to **706** in FIG. **8** as depicted by the arrow **703**. If on the other hand, the step **704** indicates that the received biometric signal does not belong to an administrator then the process **700** is directed by a NO arrow to **707** in FIG. **7**.

FIG. **7** shows the access process **600** by which a biometric signal **102** (see FIG. **2**) is processed in order to provide access to the controlled item **111**, or to take other action. Entering the process at **707** from FIG. **6**, the process **600** proceeds to a step **602** that compares the received biometric signature to signatures stored in the database **105**. A following step **603** determines if the received signal falls into the "duress" category. Signatures in this category indicate that the user **101** is in a coercive situation where, for example, an armed criminal is forcing the user **101** to access the secure facility (such as a bank door). If the step **603** determines that the signature is in the duress class, then a following step **604** prepares a "duress" bit for incorporation into the code access signal **108**. The aforementioned duress bit is an access attribute of the biometric signal **102**. Thereafter the process **600** proceeds to a step **605**.

Modules used in the code entry module for producing the rolling code enable a number of user defined bits to be inserted into the access signal **108**, and these bits can be used to effect desired control functions in the receiver sub-system **117**. The disclosed system **100** utilises four such user bits, namely (a) to indicate that the user belongs to the duress category, (b) to indicate a "battery low" condition, or other desired system state or "telemetry" variable, for the code entry module **103**, (c) to indicate that the biometric signal represents a legitimate user in which case the secure access to the controlled item **111** is to be granted, or (d) to indicate that the biometric signal is unknown, in which case the controller **109** in the receiver sub-system **117** sounds an alert tone using a bell (not shown) or the like.

Returning to FIG. **7**, if the step **603** determines that the biometric signal is not in the duress class, then the process **600** proceeds according to a NO arrow to the step **605**. The step **605** determines if the code entry module **103** has a low battery condition, in which event the process **600** proceeds according to a YES arrow to a step **606** that prepares a telemetry bit for insertion into the access signal **108**. The aforementioned telemetry bit is an access attribute of the biometric signal **102**. Thereafter, the process proceeds to a step **607**.

If the step **605** determines that telemetry signalling is not required, then the process **600** proceeds according to a NO arrow to the step **607**. The step **607** checks the biometric signal against the signatures in the database **105**. If the received biometric signal matches a legitimate signature in the database **105**, then the process is directed to a step **608** that prepares an "access" bit for insertion into the access signal **108**. This access bit directs the controller **109** in the receiver sub-system **117** to provide access to the controlled item **111**. The aforementioned access bit is an access attribute of the biometric signal **102**. The process **600** then proceeds to a step **610**.

If the step **607** determines that the biometric input signal does not match any legitimate signatures in the database **105**, then the process **600** proceeds according to a NO arrow to a step **609** that prepares an "alert" bit for insertion into the access signal **108**. The aforementioned alert bit is an access attribute of the biometric signal **102**. This alert bit directs the controller **109** (a) not to provide access to the controlled item **111**, and (b) to provide an alert tone, like ringing a chime or a bell (not shown), to alert personnel in the vicinity of the receiver sub-system **117** that an unauthorised user is attempting to gain access to the controlled item **111**. The alert bit can also cause a camera mounted near the controlled item **111** to photograph the unauthorised user for later identification of that person. The camera can be activated if the person attempting to gain access is unauthorised, and also if the person attempting to gain access is authorised but uses a duress signature.

An optional additional step (not shown) can prepare an identification field for insertion into the access signal **108**. This sends, to the receiver sub-system **117**, ID information that the receiver sub-system can use to construct an audit trail listing which users, having signatures in the database **105**, have been provided with access to the controlled item **111**.

The process **600** is then directed to the step **610** which inserts the various user defined bits into the access signal **108** and sends the signal **108** to the receiver sub-system **117**. Thereafter, the process **600** is directed by an arrow **611** to **705** in FIG. **6**.

FIG. **8** shows a process **800** for implementing various enrolment procedures. The process **800** commences at **706** from FIG. **6** after which a step **801** determines if the biometric signal is a first administrators input (which is the case if the database **105** is empty). If this is the case, then the process **800** is directed to a step **802** that stores the administrator's signature in the database **105**. From a terminology perspective, this first administrator, or rather the first administrator's first finger (in the event that the biometric sensor **121** in FIG. **2** is a fingerprint sensor), is referred to as the "superfinger". Further administrator's fingers are referred to as admin-fingers, and ordinary users fingers are referred to merely as "fingers". The reason that someone would enrol more than one of their own fingers into the system is to ensure that even in the event that one of their enrolled fingers is injured, the person can still operate the system using another enrolled finger.

It is noted that the step **802**, as well as the steps **805**, **807** and **809** involve sequences of finger presses on the biometric sensor **121** in conjunction with feedback signals from the LEDs **122** and/or the audio speaker **124**. The process **800** then proceeds to a step **810** that determines if further enrolment procedures are required. If this is the case, then the process **800** proceeds by a YES arrow back to the step **801**. If no further enrolment procedures are required, then the process **800** proceeds by a NO arrow to **705** in FIG. **6**.

Returning to the step **801**, if the biometric signal is not a first administrator's signal, then the process **800** proceeds by a NO arrow to a step **803**. The step **803** determines if a further administrator signature is to be stored. It is noted that all

signatures stored in the database are tagged as belonging to one or more of the classes of administrator, ordinary user, and duress users. If a further administrator signature is to be stored, then the process **800** proceeds by a YES arrow to the step **802** that stores the biometric signal as a further administrator's signature.

If a further administrator's signature is not required, then the process **800** proceeds according to a NO arrow to a step **804** that determines if a duress signature is to be stored. If this is the case then the process **800** follows a YES arrow to a step **805** that stores a duress signature. The process **800** then proceeds to the step **810**. If however the step **804** determines that a duress signature is not required, then the process **800** proceeds by a NO arrow to s step **806**.

The step **806** determines if a further simple signature (i.e. belonging to an ordinary user) is to be stored. If a further simple signature is to be stored, then the process **800** proceeds by a YES arrow to the step **807** that stores the biometric signal as a further ordinary signature.

If a further simple signature is not required, then the process **800** proceeds according to a NO arrow to a step **808** that determines if any or all signatures are to be erased from the database **105**. If this is the case then the process **800** follows a YES arrow to a step **809** that erases the desired signatures. The process **800** then proceeds to the step **810**. If however the step **804** determines that no signatures are to be erased, then the process **800** proceeds by a NO arrow to the step **810**.

FIG. **9** shows another enrolment process relating to the example of FIG. **6**. The process **900** commences at **706** from FIG. **6** after which a step **901** determines if the received biometric signal comes from the first administrator. If this is the case, then the process **900** proceeds according to a YES arrow to a step **902**. The step **902** emits an "Enrolment" tone and flashes the green LED once only. Thereafter, a step **905** reads the incoming biometric signal which is provided by the user as directed by the Amber LED. When the Amber LED flashes continuously, this directs the user to "Apply Finger". When the Amber LED is in a steady illuminated state, this directs the user to "Maintain Finger Pressure". Finally, when the amber LED is off, this directs the user to "Remove Finger".

Returning to the step **901**, if the incoming biometric signal does not belong to the first administrator, then the process **900** proceeds according to a NO arrow to a step **903**. The step **903** emits an "Enrolment" tone, and flashes the Red LED in an on-going fashion. Thereafter, the process **900** proceeds according to an arrow **904** to the step **905**.

Following the step **905**, a step **906** determines whether the incoming biometric signal is legible. If this is not the case, then the process **900** proceeds according to a NO arrow to a step **907**. The step **907** emits a "Rejection" tone, after which the process **900** is directed, according to an arrow **908** to **705** in FIG. **6**. Returning to the step **906**, if the incoming biometric signal is legible, then the process **900** follows a YES arrow to a step **909**. The step **909** determines whether the finger press exceeds a predetermined time. If this is not the case, then the process **900** follows a NO arrow to a step **910** which stores the biometric signal, which in the present case is a fingerprint signature. Thereafter the process **900** follows an arrow **911** to **705** in FIG. **6**.

Returning to the step **909** if the finger press does exceed the predetermined period, then the process follows a YES arrow to a step **912**. The step **912** erases relevant signatures depending upon the attributes of the incoming biometric signal. Thus, for example, if the incoming biometric signal belongs to an ordinary user, then the ordinary user's signature in the database **105** is erased by the step **912**. If, on the other hand, the incoming biometric signal belongs to the first administrator, then all the signatures in the database **105** are erased. Administrators who are not the first administrator can be granted either the same powers as the first administrator in regard to erasure of signatures, or can be granted the same powers as ordinary user in this respect.

Once the step **912** has completed erasure of the relevant signatures, then the process **900** follows an arrow **913** to **705** in FIG. **6**.

FIG. **10** is a schematic block diagram of the system in. FIG. **2**. The disclosed secure access methods are preferably practiced using a computer system arrangement **100'**, such as that shown in FIG. **10** wherein the processes of FIGS. **3-4**, and **6-9** may be implemented as software, such as application program modules executing within the computer system **100'**. In particular, the method steps for providing secure access are effected by instructions in the software that are carried out under direction of the respective processor modules **107** and **109** in the transmitter and receiver sub-systems **116** and **117**. The instructions may be formed as one or more code modules, each for performing one or more particular tasks. The software may also be divided into two separate parts, in which a first part performs the provision of secure access methods and a second part manages a user interface between the first part and the user. The software may be stored in a computer readable medium, including the storage devices described below, for example. The software is loaded into the transmitter and receiver sub-systems **116** and **117** from the computer readable medium, and then executed under direction of the respective processor modules **107** and **109**. A computer readable medium having such software or computer program recorded on it is a computer program product. The use of the computer program product in the computer preferably effects an advantageous apparatus for provision of secure access.

The following description is directed primarily to the transmitter sub-system **116**, however the description applies in general to the operation of the receiver sub-system **117**. The computer system **100'** is formed, having regard to the transmitter sub-system **116**, by the controller module **107**, input devices such as the bio sensor **121**, output devices including the LED display **122** and the audio device **124**. A communication interface/transceiver **1008** is used by the controller module **107** for communicating to and from a communications network **1020**. Although FIG. **2** shows the transmitter sub-system **116** communicating with the receiver sub-system **117** using a direct wireless link for the access signal **108**, this link used by the access signal **108** can be effected over the network **1020** forming a tandem link comprising **108-1020-108'**. The aforementioned communications capability can be used to effect communications between the transmitter sub-system **116** and the receiver sub-system **117** either directly or via the Internet, and other network systems, such as a Local Area Network (LAN) or a Wide Area Network (WAN).

The controller module **107** typically includes at least one processor unit **1005**, and a memory unit **1006**, for example formed from semiconductor random access memory (RAM) and read only memory (ROM). The controller module **107** also includes an number of input/output (I/O) interfaces including an audio-video interface **1007** that couples to the LED display **122** and audio speaker **124**, an I/O interface **1013** for the bio-sensor **121**, and the interface **1008** for communications. The components **1007**, **1008**, **1005**, **1013** and **1006** the controller module **107** typically communicate via an interconnected bus **1004** and in a manner which results in a conventional mode of operation of the controller **107** known to those in the relevant art.

Typically, the application program modules for the transmitter sub-system **116** are resident in the memory **1006** iROM, and are read and controlled in their execution by the processor **1005**. Intermediate storage of the program and any data fetched from the bio sensor **121** and the network **1020** may be accomplished using the RAM in the semiconductor memory **1006**. In some instances, the application program modules may be supplied to the user encoded into the ROM in the memory **1006**. Still further, the software modules can also be loaded into the transmitter sub-system **116** from other computer readable media, say over the network **1020**. The term "computer readable medium" as used herein refers to any storage or transmission medium that participates in providing instructions and/or data to the transmitter sub-system **116** for execution and/or processing. Examples of storage media include floppy disks, magnetic tape, CD-ROM, a hard disk drive, a ROM or integrated circuit, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the transmitter sub-system **116**. Examples of transmission media include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

INDUSTRIAL APPLICABILITY

It is apparent from the above that the arrangements described are applicable to the security industry.

The foregoing describes only some embodiments of the present invention, and modifications and/or changes can be made thereto without departing from the scope and spirit of the invention, the embodiments being illustrative and not restrictive.

The system **100** can also be used to provide authorised access to lighting systems, building control devices, exterior or remote devices such as air compressors and so on. The concept of "secure access" is thus extendible beyond mere access to restricted physical areas.

What is claimed is:

1. A system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a transmitter sub-system comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

means for emitting a secure access signal conveying information dependent upon said accessibility attribute; and

a receiver sub-system comprising:

means for receiving the transmitted secure access signal; and

means for providing conditional access to the controlled item dependent upon said information,

wherein the transmitter sub-system further comprises means for populating the data base of biometric signatures, the population means comprising:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for populating the data base according to the instruction,

wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

2. The system according to claim **1**, further comprising:

means for providing a signal for directing input of the series of entries of the biometric signal;

means for incorporating into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database; and

means for constructing an audit trail of biometric signals provided to the biometric sensor for the purpose of accessing the controlled item.

3. The system according to claim **1**, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class, the accessibility attribute preferably comprising:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

4. The system according to claim **1**, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration, and/or the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

5. The system according to claim **1**, wherein said conditional access comprises one of:

provision of access to the controlled item if the accessibility attribute comprises an access attribute:

provision of access to the controlled item and sounding of an alert if the accessibility attribute comprises a duress attribute; and

denial of access to the controlled item and sounding of an alert if the accessibility attribute comprises an alert attribute.

6. The system as claimed in claim **1**, wherein:

the biometric sensor is for authenticating the identity of a user;

the means for emitting comprises a transmitter for transmitting information capable of granting more than two types of access to the controlled item using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and

the system further comprising a control panel for receiving the information and for providing the secure access requested.

7. The system according to claim **6**, wherein the control panel includes a converter for receiving the secure wireless signal and for outputting the information, and/or the biometric sensor authenticates the identity of the user by comparing a biometric input from the user with a biometric signature for the user in a biometric database, and/or the biometric sensor, the biometric database, and the transmitter are located in a remote fob.

8. The system according to claim **7**, wherein the secure wireless signal comprises an RF carrier and a rolling code, and the converter preferably converts the rolling code to the Wiegand protocol.

9. A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and

means for emitting a secure access signal conveying said information dependent upon said accessibility attribute;

wherein the transmitter sub-system further comprises means for populating the database of biometric signatures, the populating means comprising:

means for receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

means for mapping said series into an instruction; and

means for populating the database according to the instruction,

wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

10. A method for providing secure access to a controlled item in a system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal capable of granting more than two types of access to the controlled item, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon information in said secure access signal, the method comprising the steps of:

populating the database of biometric signatures by:

receiving a series of entries of the biometric signal;

determining at least one of the number of said entries and a duration of each said entry;

mapping said series into an instruction; and

populating the database according to the instruction;

receiving a biometric signal;

matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;

emitting a secure access signal conveying information dependent upon said accessibility attribute; and

providing conditional access to the controlled item dependent upon said information,

wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

11. The method according to claim **10**, wherein the step of populating the database of biometric signatures further comprises the step of enrolling a biometric signature into the database of biometric signatures comprising the steps of:

receiving a biometric signal; and

enrolling the biometric signal as an administrator signature if the database of biometric signatures is empty.

12. The method according to claim **11**, wherein the step of enrolling the biometric signature further comprises receiving another biometric signal to confirm the enrolling of the biometric signal as an administrator signature, and is preferably performed dependent upon generation of a feedback signal adapted to direct provision of at least one of the biometric signal and the other biometric signal.

13. A non-transitory computer readable storage medium for storing a computer program comprising instructions, which when executed by processors causes the processors to perform the steps of the method of claim **10**.

* * * * *

US009665705B2

(12) **United States Patent**
Burke

(10) **Patent No.: US 9,665,705 B2**
(45) **Date of Patent: *May 30, 2017**

(54) **REMOTE ENTRY SYSTEM**

(71) Applicant: **Securicom (NSW) Pty. Ltd.**, Ramsgate, NSW (AU)

(72) Inventor: **Christopher John Burke**, Ramsgate (AU)

(73) Assignee: **SECURICOM (NSW) PTY LTD**, Ramsgate (AU)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/000,818**

(22) Filed: **Jan. 19, 2016**

(65) **Prior Publication Data**

US 2016/0132672 A1 May 12, 2016

Related U.S. Application Data

(63) Continuation of application No. 13/572,166, filed on Aug. 10, 2012, now Pat. No. 9,269,208, which is a (Continued)

(30) **Foreign Application Priority Data**

Aug. 13, 2003 (AU) 2003904317

(51) **Int. Cl.**

H04L 29/06	(2006.01)
G06F 21/32	(2013.01)
G06F 21/35	(2013.01)
G07C 9/00	(2006.01)
H04W 12/08	(2009.01)

(Continued)

(52) **U.S. Cl.**

CPC ***G06F 21/32*** (2013.01); ***G06F 21/35*** (2013.01); ***G07C 9/00158*** (2013.01); ***H04L 63/0861*** (2013.01); ***H04W 12/08*** (2013.01); *H04W 84/12* (2013.01); *H04W 84/18* (2013.01)

(58) **Field of Classification Search**

CPC G06F 21/32

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,109,428 A *	4/1992	Igaki	.....	A61B 5/1172 356/71
5,933,515 A *	8/1999	Pu	.....	G06K 9/00006 340/5.53
7,152,045 B2 *	12/2006	Hoffman	.....	G06F 21/32 235/379

OTHER PUBLICATIONS

Klosterman, Andrew J., and Gregory R. Ganger. "Secure continuous biometric-enhanced authentication." (2000).*

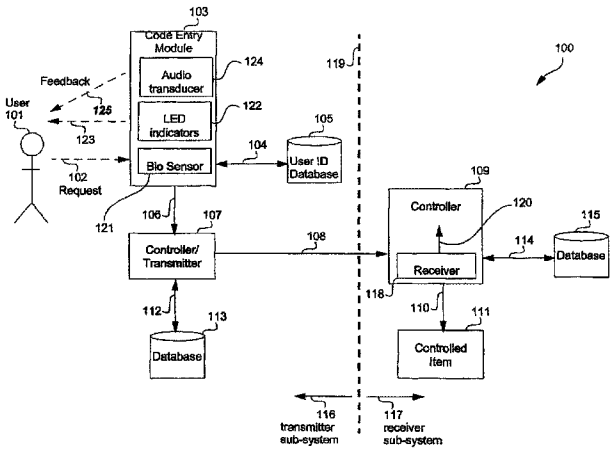
* cited by examiner

Primary Examiner — Shawnchoy Rahman
(74) *Attorney, Agent, or Firm* — Brinks Gilson & Lione

(57) **ABSTRACT**

A system is disclosed for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol, and a receiver sub-system comprising means for receiving the transmitted secure access signal and means for providing conditional access to the controlled item dependent upon said information.

17 Claims, 10 Drawing Sheets



Related U.S. Application Data

continuation of application No. 10/568,207, filed as application No. PCT/AU2004/001083 on Aug. 13, 2004, now Pat. No. 8,266,442.

(51) **Int. Cl.**

H04W 84/12	(2009.01)
H04W 84/18	(2009.01)

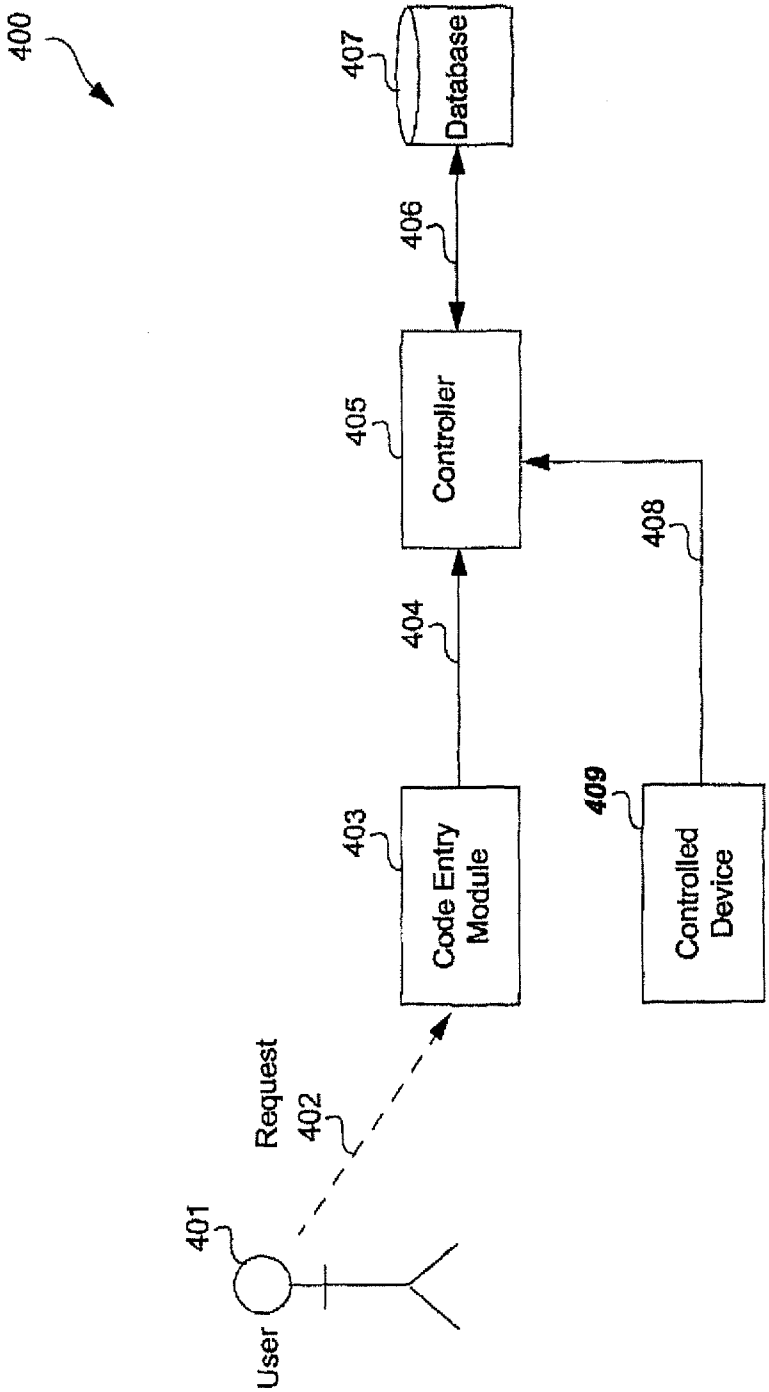


Fig. 1
(prior art)

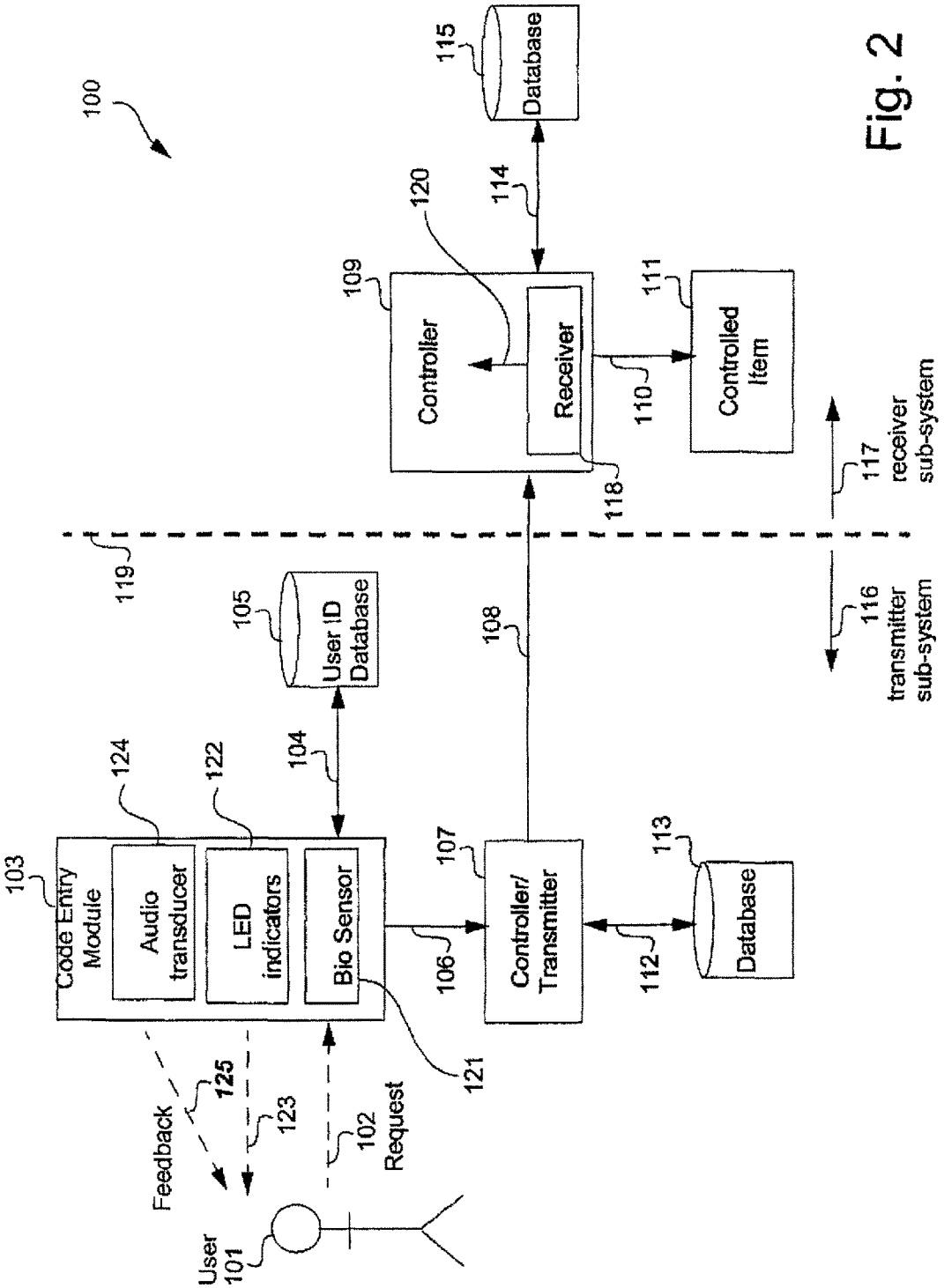


Fig. 2

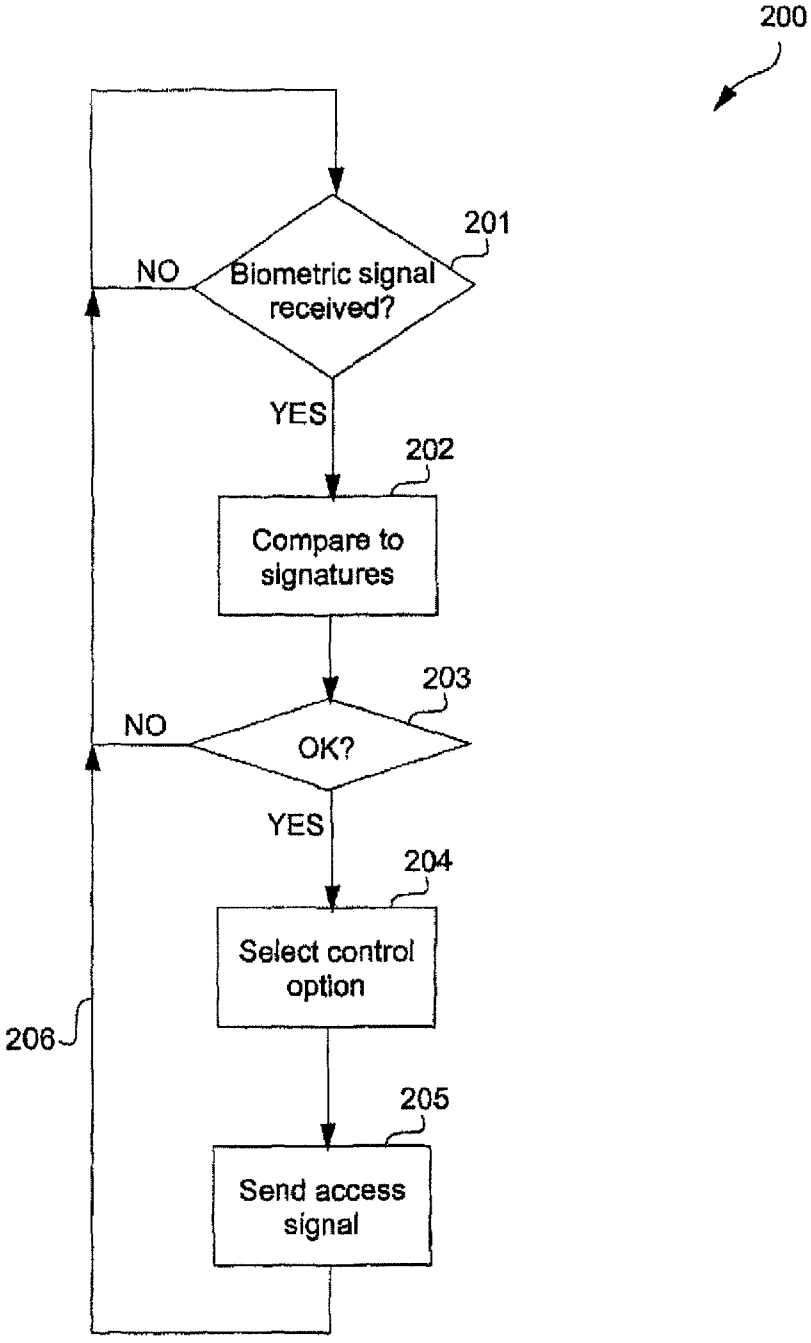

200
201
Biometric signal received?
NO
YES
202
Compare to signatures
203
OK?
NO
YES
204
Select control option
205
Send access signal
206

Fig. 3

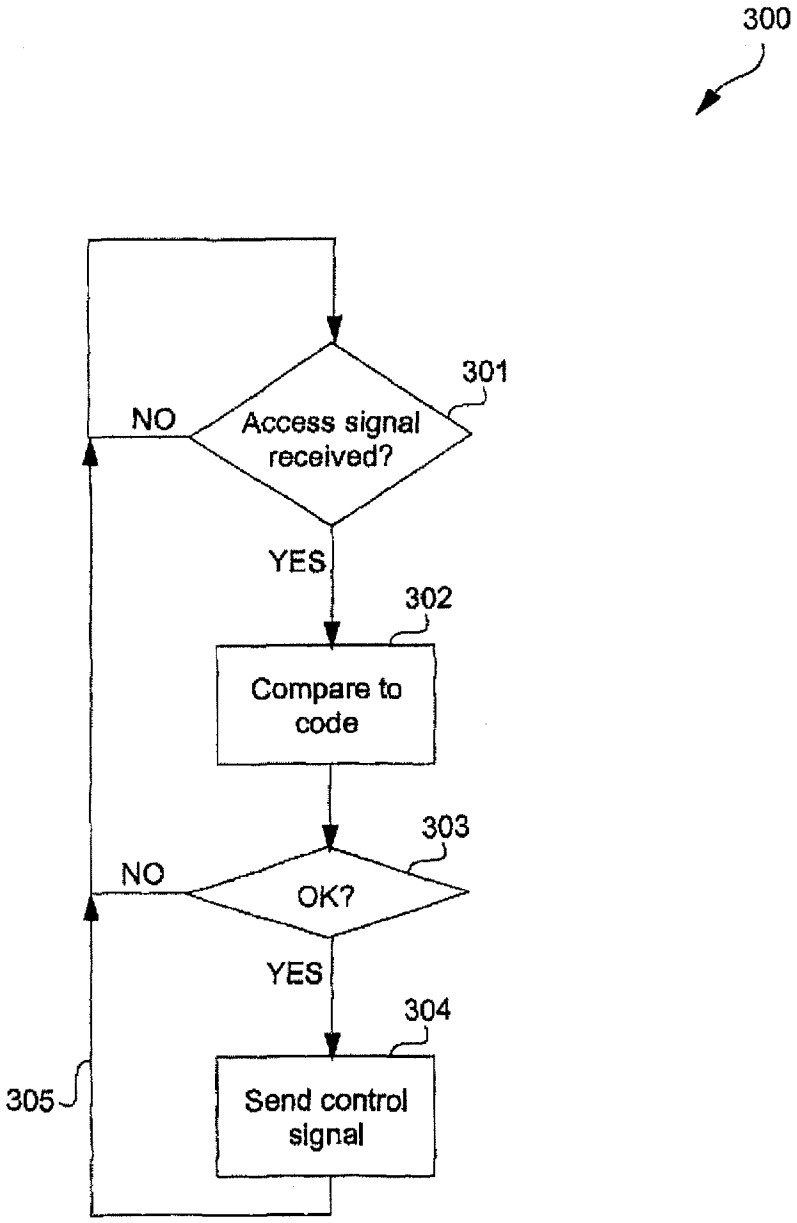
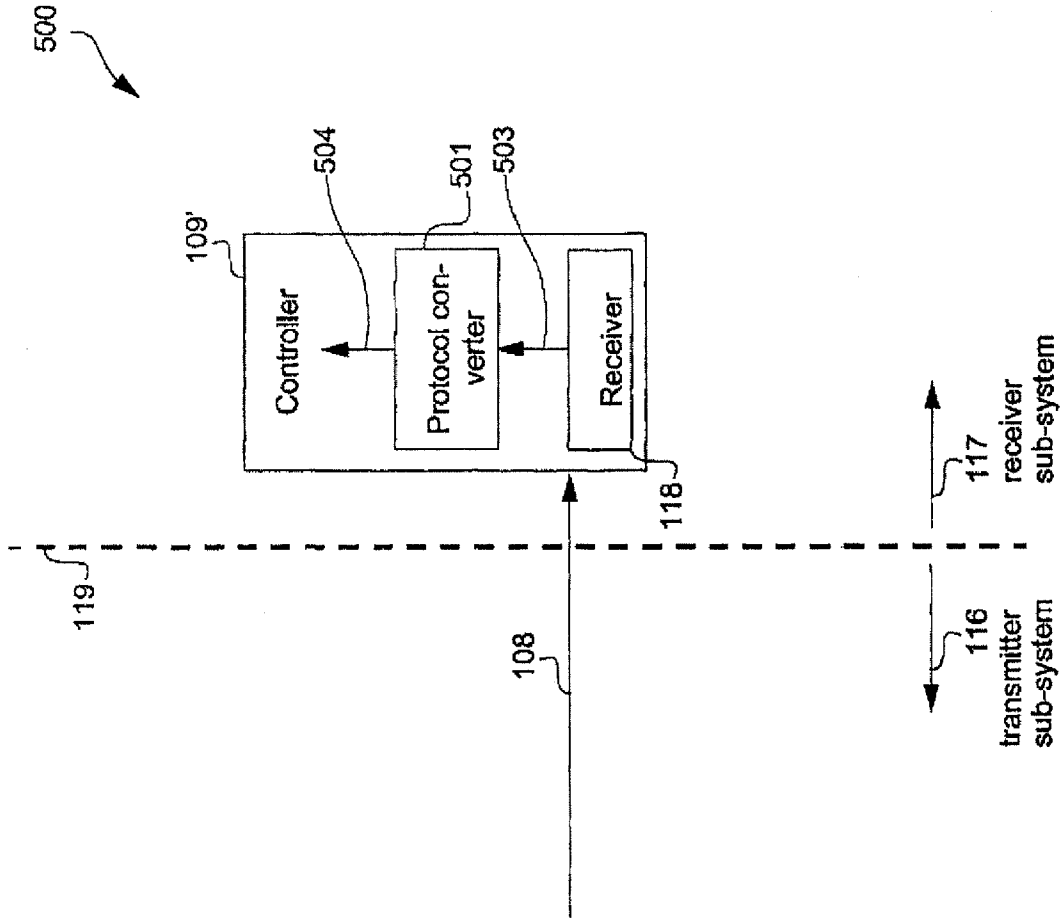

300
301
Access signal received?
NO
YES
302
Compare to code
303
OK?
NO
YES
304
Send control signal
305

Fig. 4

Fig. 5


500
109'
504
501
503
Controller
Protocol con-verter
Receiver
118
117
receiver sub-system
119
108
116
transmitter sub-system

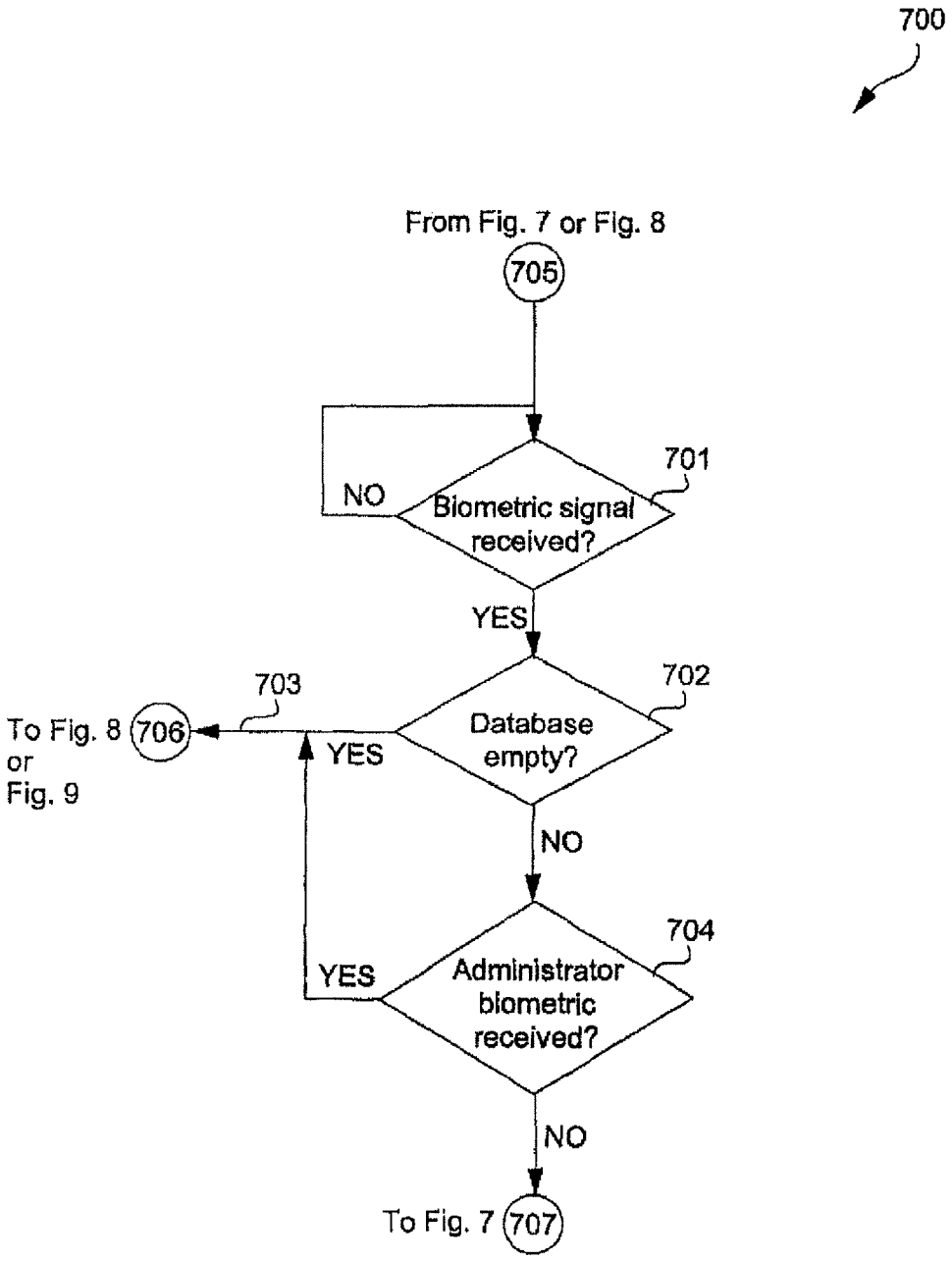

700
From Fig. 7 or Fig. 8
705
701
NO
Biometric signal received?
YES
703
702
To Fig. 8 or Fig. 9
706
YES
Database empty?
NO
704
YES
Administrator biometric received?
NO
To Fig. 7
707

Fig. 6

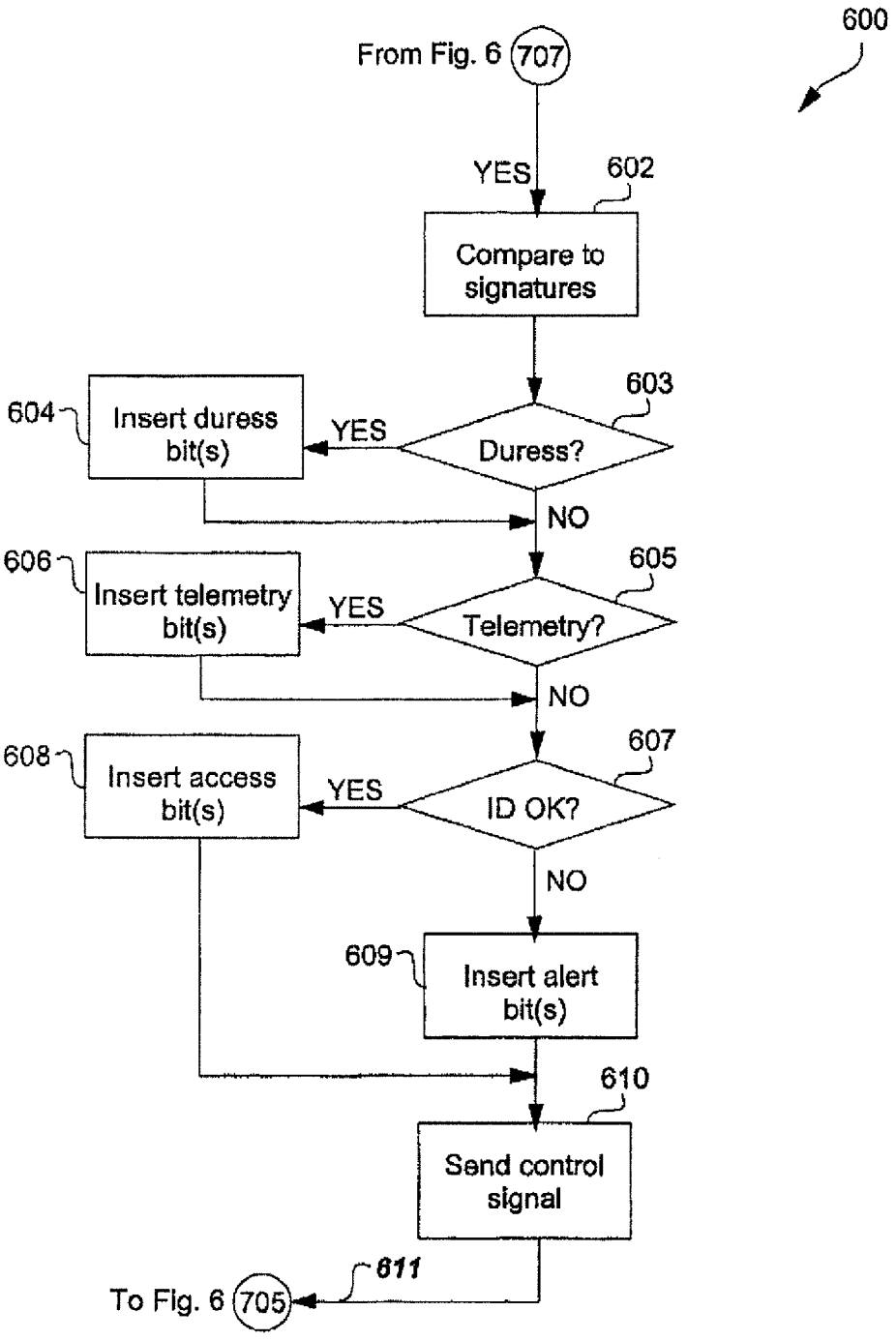

600
From Fig. 6 707
YES
602
Compare to signatures
603
604
Insert duress bit(s)
YES
Duress?
NO
606
Insert telemetry bit(s)
YES
605
Telemetry?
NO
608
Insert access bit(s)
YES
607
ID OK?
NO
609
Insert alert bit(s)
610
Send control signal
611
To Fig. 6 705

Fig. 7

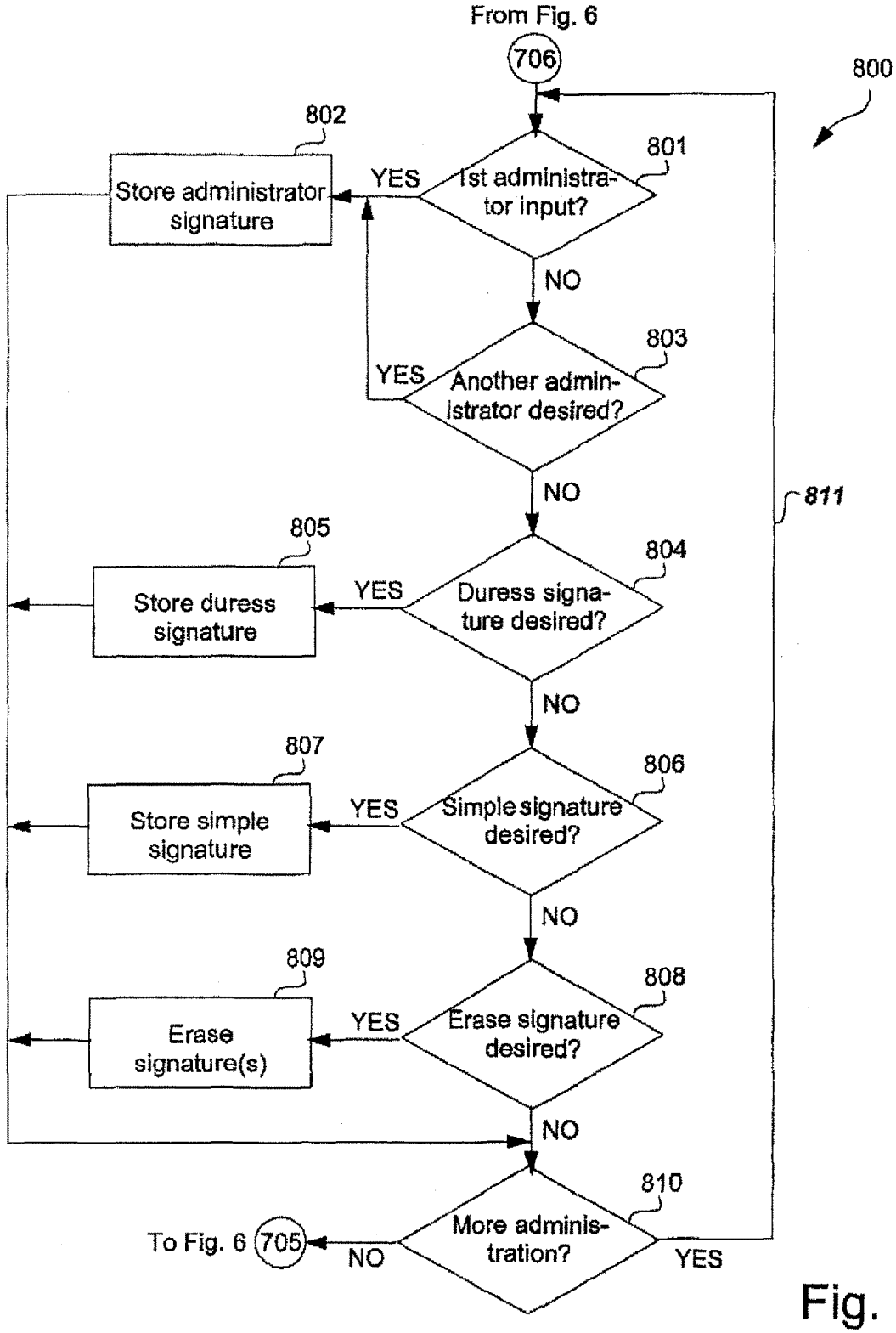

From Fig. 6
706
800
802
801
Store administrator signature
YES
1st administrator input?
NO
803
YES
Another administrator desired?
NO
811
805
804
Store duress signature
YES
Duress signature desired?
NO
807
806
Store simple signature
YES
Simple signature desired?
NO
809
808
Erase signature(s)
YES
Erase signature desired?
NO
810
To Fig. 6 705
NO
More administration?
YES

Fig. 8

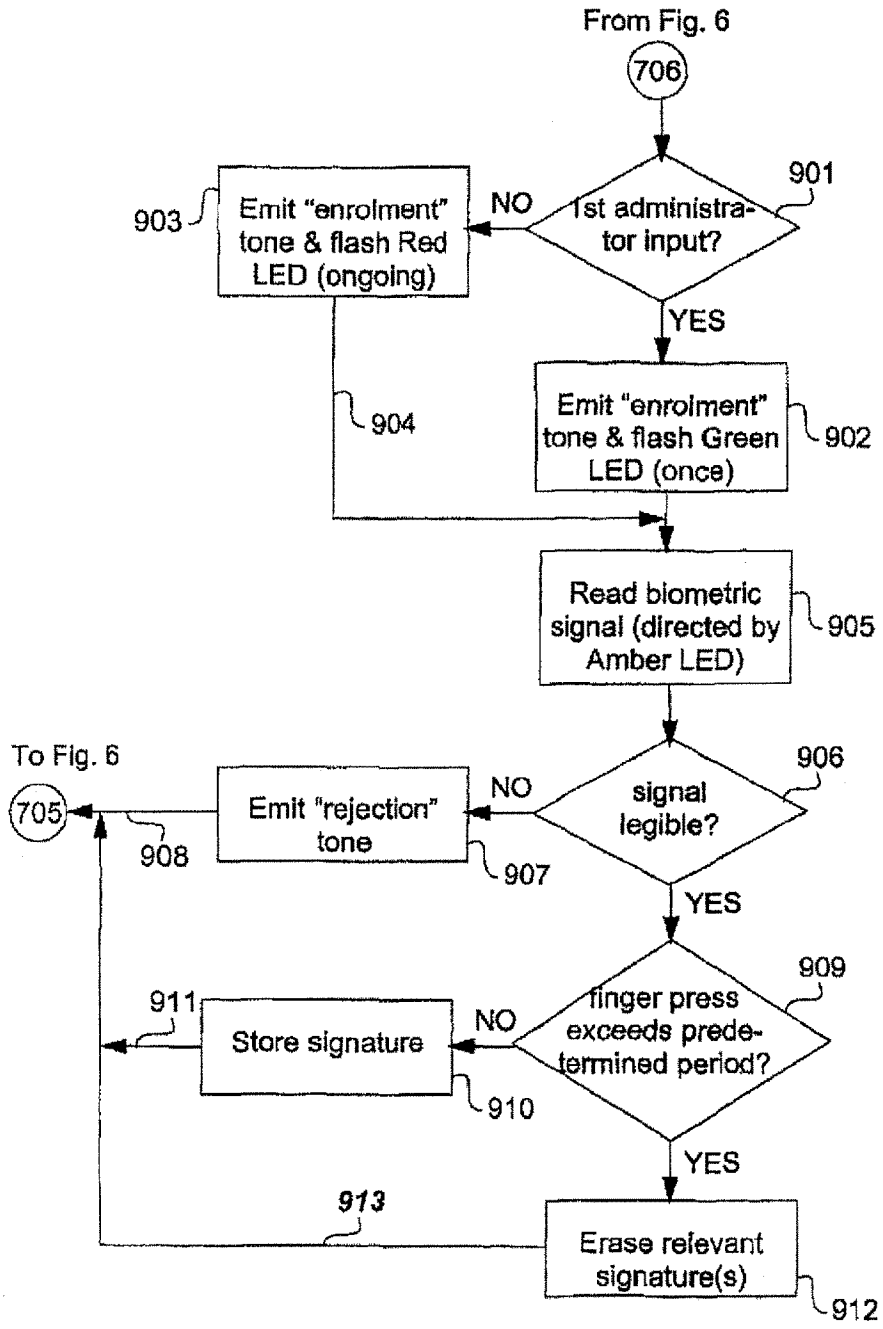

From Fig. 6
706
900
901
1st administrator input?
NO
903
Emit "enrolment" tone & flash Red LED (ongoing)
YES
904
Emit "enrolment" tone & flash Green LED (once)
902
Read biometric signal (directed by Amber LED)
905
To Fig. 6
705
906
signal legible?
NO
Emit "rejection" tone
908
907
YES
909
finger press exceeds predetermined period?
911
NO
Store signature
910
YES
913
Erase relevant signature(s)
912

Fig. 9

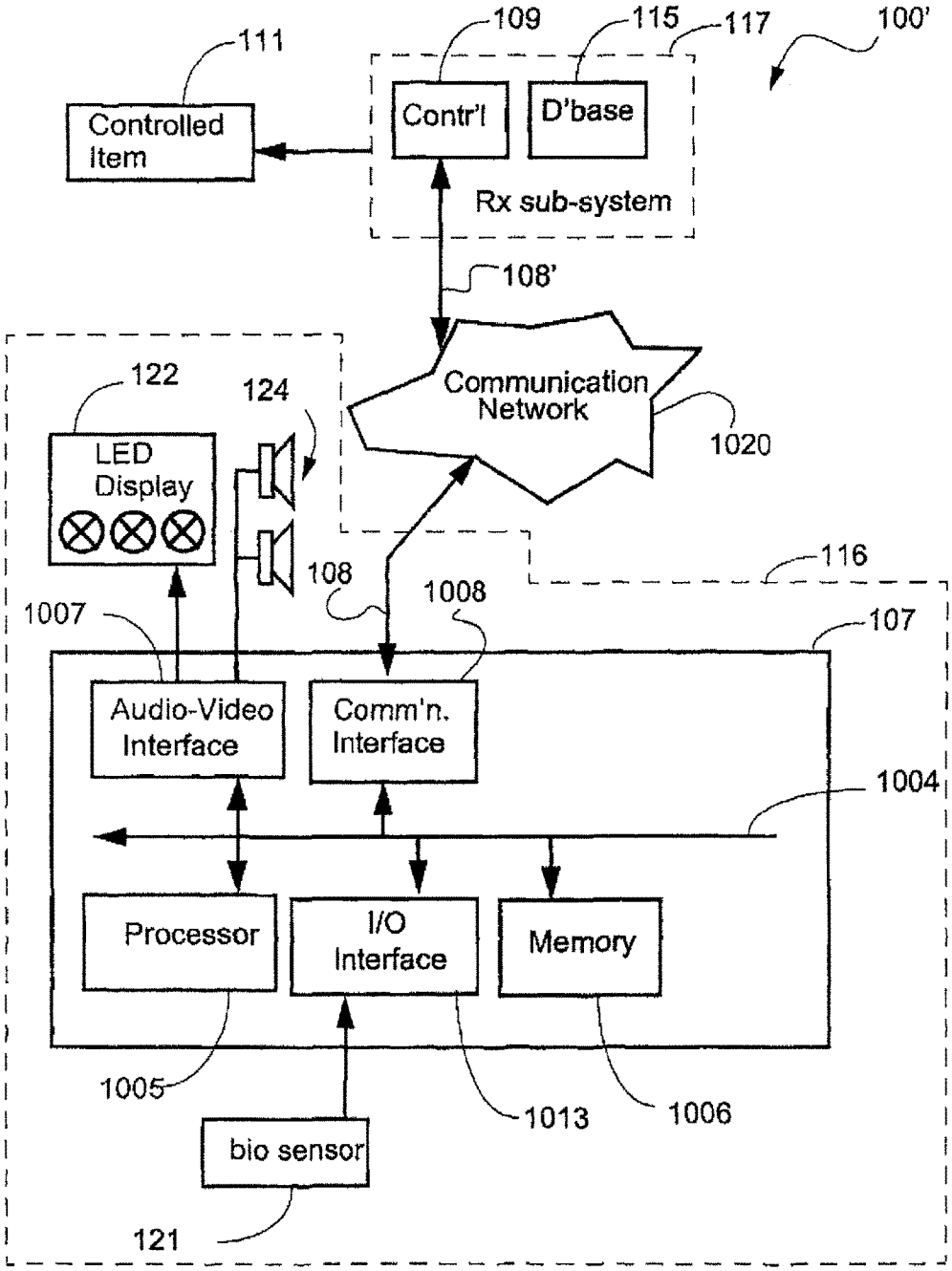

111
109
115
117
100'
Controlled Item
Contr'l
D'base
Rx sub-system
108'
Communication Network
1020
122
124
LED Display
108
116
1008
1007
107
Audio-Video Interface
Comm'n. Interface
1004
Processor
I/O Interface
Memory
1005
1013
1006
bio sensor
121

Fig. 10

REMOTE ENTRY SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation patent application of U.S. Non-Provisional application Ser. No. 10/568,207 for REMOTE ENTRY SYSTEM, filed Jun. 4, 2008, the disclosure of which is incorporated by reference in its entirety.

FIELD OF THE INVENTION

The present invention relates to secure access systems and, in particular, to systems using wireless transmission of security code information.

BACKGROUND

FIG. **1** shows a prior art arrangement for providing secure access. A user **401** makes a request, as depicted by an arrow **402**, directed to a code entry module **403**. The module **403** is typically mounted on the external jamb of a secure door. The request **402** is typically a secure code of some type which is compatible with the code entry module **403**. Thus, for example, the request **402** can be a sequence of secret numbers directed to a keypad **403**. Alternately, the request **402** can be a biometric signal from the user **401** directed to a corresponding biometric sensor **403**. One example of a biometric signal is a fingerprint. Other physical attributes that can be used to provide biometric signals include voice, retinal or iris pattern, face pattern, palm configuration and so on.

The code entry module **403** conveys the request **402** by sending a corresponding signal, as depicted by an arrow **404**, to a controller **405** which is typically situated in a remote or inaccessible place. The controller **405** authenticates the security information provided by the user **401** by interrogating a database **407** as depicted by an arrow **406**. If the user **401** is authenticated, and has the appropriate access privileges, then the controller **405** sends an access signal, as depicted by an arrow **408**, to a device **409** in order to provide the desired access. The device **409** can, for example, be the locking mechanism of a secure door, or can be an electronic lock on a personal computer (PC) which the user **401** desires to access.

A proximity card can also be used to emit the request **402**, in which case the code entry module **403** has appropriate functionality.

Although the request **402** can be made secure, either by increasing the number of secret digits or by using a biometric system, the communication infrastructure in FIG. **1** is typically less secure. The infrastructure **400** is generally hardwired, with the code entry module **403** generally being mounted on the outside jamb of a secured door. In such a situation, the signal path **404** can be over a significant distance in order to reach the controller **405**. The path **404** represents one weak point in the security system **400**, providing an unauthorised person with relatively easy access to the information being transmitted between the code entry module **403** and the controller **405**. Such an unauthorised person can, given this physical access, decipher the communicated information between the code entry module **403** and the controller **405**. This captured information can be deciphered, replayed in order to gain the access which rightfully belongs to the user **401**, or to enable modification for other subversive purposes.

Current systems as depicted in FIG. **1** utilise a communication protocol called "Wiegand" for communication between the code entry module **403** and the controller **405**. The Wiegand protocol is a simple one-way data protocol that can be modified by increasing or decreasing the bit count to ensure uniqueness of the protocol among different security companies. The Wiegand protocol does not secure the information being sent between the code entry module **403** and the controller **405**.

More advanced protocols such as RS 485 have been used in order to overcome the vulnerability of the Wiegand protocol over the long distance route **404**. RS 485 is a duplex protocol offering encryption capabilities at both the transmitting and receiving ends, i.e. the code entry module **403** and the controller **405** respectively in the present case. The length of the path **404** nonetheless provides an attack point for the unauthorised person.

Due to the cost and complexity of re-wiring buildings and facilities, security companies often make use of existing communication cabling when installing and/or upgraded security systems, thereby maintaining the vulnerability described above.

SUMMARY

It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

According to a first aspect of the present invention, there is provided a system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a transmitter subsystem comprising: a biometric sensor for receiving a biometric signal; means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; and

a receiver sub-system comprising; means for receiving the transmitted secure access signal; and means for providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a transmitter sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a receiver sub-system comprising means for receiving a secure access signal transmitted by the transmitter subsystem, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal; wherein the transmitter subsystem comprises: a biometric sensor for receiving a biometric signal; means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and means for emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol.

According to another aspect of the present invention, there is provided receiver sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for

receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; wherein the receiver sub-system comprises; means for receiving the transmitted secure access signal; and means for providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a method for providing secure access to a controlled item, the method comprising the steps of:

receiving a biometric signal;

matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute;

emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; and

providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a method for populating a database of biometric signatures in a system for providing secure access to a controlled item, the system comprising said database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal, and a receiver subsystem comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon information in said secure access signal, said method comprising the steps of:

receiving a series of entries of the biometric signal;

determining at least one of the number of said entries and a duration of each said entry;

mapping said series into an instruction; and

populating the database according to the instruction.

According to another aspect of the present invention, there is provided a method for transmitting a secure access signal in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a receiver sub-system comprising means for receiving the secure access signal transmitted by a transmitter subsystem, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal, said method comprising the steps of: receiving a biometric sensor by biometric signal; matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol.

According to another aspect of the present invention, there is provided a method for receiving a secure access signal in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute, and means for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol, said method comprising the steps of:

receiving the transmitted secure access signal; and providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to provide secure access to a controlled item, said computer program product comprising:

code for receiving a biometric signal;

code for matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute;

code for emitting a secure access signal conveying information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol; and

code for providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to populate a database of biometric signatures in a system for providing secure access to a controlled item, said computer program product comprising:

code for receiving a series of entries of the biometric signal;

code for determining at least one of the number of said entries and a duration of each said entry;

code for mapping said series into an instruction; and

code for populating the database according to the instruction.

According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to transmit a secure access signal in a system for providing secure access to a controlled item, said computer program product comprising:

code for receiving a biometric sensor by biometric signal;

code for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

code for emitting the secure access signal conveying said information dependent upon said accessibility attribute, wherein the secure access signal comprises one of at least a rolling code, an encrypted Bluetooth™ protocol, and a WiFi™ protocol.

According to another aspect of the present invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for directing a processor to receive a secure access signal in a system for providing secure access to a controlled item, said computer program product comprising:

code for receiving the transmitted secure access signal; and

code for providing conditional access to the controlled item dependent upon said information.

According to another aspect of the present invention, there is provided a system for providing secure access, the system comprising:

a biometric sensor for authenticating the identity of a user;

a transmitter for transmitting information using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and

a control panel for receiving the information and for providing the secure access requested.

Other aspects of the invention are also disclosed.

BRIEF DESCRIPTION OF THE DRAWINGS

Some aspects of the prior art and one or more embodiments of the present invention are described with reference to the drawings, in which:

FIG. **1** shows a prior art arrangement for providing secure access;

FIG. **2** is a functional block diagram of an arrangement for providing secure access according to the present disclosure;

FIG. **3** shows an example of a method of operation of the remote control module of FIG. **2**;

FIG. **4** shows an example of a method of operation of the (fixed) control device of FIG. **2**;

FIG. **5** shows incorporation of a protocol converter into the arrangement of FIG. **2**; and

FIG. **6** shows another example of how the remote access system operates;

FIG. **7** shows an access process relating to the example of FIG. **6**;

FIG. **8** shows one enrollment process relating to the example of FIG. **6**;

FIG. **9** shows another enrollment process relating to the example of FIG. **6**; and

FIG. **10** is a schematic block diagram of the system in FIG. **2**.

DETAILED DESCRIPTION INCLUDING BEST MODE

It is to be noted that the discussions contained in the "Background" section relating to prior art arrangements relate to discussions of documents or devices which form public knowledge through their respective publication and/or use. Such should not be interpreted as a representation by the present inventor(s) or patent applicant that such documents or devices in any way form part of the common general knowledge in the art.

Where reference is made in any one or more of the accompanying drawings to steps and/or features, which have the same reference numerals, those steps and/or features have for the purposes of this description the same function(s) or operation(s), unless the contrary intention appears.

FIG. **2** is a functional block diagram of an arrangement for providing secure access according to the present disclosure. A user **101** makes a request, as depicted by an arrow **102**, to a code entry module **103**. The code entry module **103** includes a biometric sensor **121** and the request **102** takes a form which corresponds to the nature of the sensor **121** in the module **103**. Thus, for example, if the biometric sensor **121** in the code entry module **103** is a fingerprint sensor, then the request **102** typically takes the form of a thumb press on a sensor panel (not shown) on the code entry module **103**.

The code entry module **103** interrogates, as depicted by an arrow **104**, a user identity database **105**. Thus for example if the request **102** is the thumb press on the biometric sensor panel **121** then the user database **105** contains biometric signatures for authorised users against which the request **102** can be authenticated. If the identity of the user **101** is authenticated successfully, then the code entry module **103** sends a signal **106** to a controller/transmitter **107**. The controller/transmitter **107** checks, as depicted by an arrow **112**, the current rolling code in a database **113**. The controller **107** then updates the code and sends the updated code, this being referred to as an access signal, as depicted by an arrow **108** to a controller **109**. The rolling code protocol offers non-replay encrypted communication.

The controller **109** tests the rolling code received in the access signal **108** against the most recent rolling code which has been stored in a database **115**, this testing being depicted by an arrow **114**. If the incoming rolling code forming the access signal **108** is found to be legitimate, then the controller **109** sends a command, as depicted by an arrow **110**, to a controlled item **111**. The controlled item **111** can be a door locking mechanism on a secure door, or an electronic key circuit in a personal computer (PC) that is to be accessed by the user **101**. It is noted that the controller **109** contains a receiver **118** that receives the transmitted access signal **108** and converts it into a form that is provided, as depicted by an arrow **120**, into a form that the controller **109** can use.

The code entry module **103** also incorporates at least one mechanism for providing feedback to the user **101**. This mechanism can, for example, take the form or one or more Light Emitting Diodes (LEDs) **122** which can provide visual feedback, depicted by an arrow **123** to the user **101**. Alternately or in addition the mechanism can take the form of an audio signal provided by an audio transducer **124** providing audio feedback **125**.

The arrangement in FIG. **2** has been described for the case in which the secure code in the access signal **108** used between the sub-systems **116** and **117** is based upon the rolling code. It is noted that this is merely one arrangement, and other secure codes can equally be used. Thus, for example, either of the Bluetooth™ protocol, or the Wi Fi™ protocols can be used.

Rolling codes provide a substantially non-replayable non-repeatable and encrypted radio frequency data communications scheme for secure messaging. These codes use inherently secure protocols and serial number ciphering techniques which in the present disclosure hide the clear text values required for authentication between the key fob (transmitter) sub-system **116** and the receiver/controller **118**/**109**.

Rolling codes use a different code variant each time the transmission of the access signal **108** occurs. This is achieved by encrypting the data from the controller **107** with a mathematical algorithm, and ensuring that successive transmissions of the access signal **108** are modified using a code and/or a look-up table known to both the transmitter sub-system **116** and the receiver sub-system **117**. Using this approach successive transmissions are modified, resulting in a non-repeatable data transfer, even if the information from the controller **107** remains the same. The modification of the code in the access signal **108** for each transmission significantly reduces the likelihood that an intruder can access the information replay the information to thereby gain entry at some later time.

The sub-system in FIG. **2** falling to the left hand side, as depicted by an arrow **116**, of a dashed line **119** can be implemented in a number of different forms. The sub-system **116** can for example be incorporated into a remote fob (which is a small portable device carried by the user **101**), or alternately can be mounted in a protected enclosure on the outside jamb of a secured door. The sub-system **116** com-

municates with the sub-system **117** on the right hand side of the dashed line **119** via the wireless communication channel used by the access signal **108**. The sub-system **117** is typically located in an inaccessible area such as a hidden roof space or alternately in a suitable protected area such as an armoured cupboard. The location of the sub-system **117** must of course be consistent with reliable reception of the wireless access signal **108**.

Although typically the communication channel uses a wireless transmission medium, there are instances where the channel used by the access signal **108** can use a wired medium. This is particularly the case when the transmitter sub-system **116** is mounted in an enclosure on the door jamb rather than in a portable key fob.

The biometric signature database **105** is shown in FIG. **2** to be part of the transmitter sub-system **116**. However, in an alternate arrangement, the biometric signature database **105** can be located in the receiver sub-system **117**, in which case the communication **104** between the code entry module **103** and the signature database **105** can also be performed over a secure wireless communication channel such as the one used by the access signal **108**. In the event that the secure access system is being applied to providing secure access to a PC, then the secured PC can store the biometric signature of the authorised user in internal memory, and the PC can be integrated into the receiver sub-system **117** of FIG. **1**.

In the event that the sub-system **116** is implemented as a remote fob, the combination of the biometric verification and the strongly encrypted wireless communication provides a particularly significant advantage over current systems. The remote key fob arrangement allows easy installation, since the wired communication path **404** (see FIG. **1**) is avoided. Other existing wiring elements of the present systems **400** can be used where appropriate. When the sub-system **116** is implemented as a remote fob, the fob incorporates the biometric (eg fingerprint) authentication arrangement, in which case only one biometric signature is stored in the fob. This arrangement reduces the requirements on the central database **115**. Once the key fob authenticates the user through biometric signature (eg fingerprint) verification, the rolling code in the access signal **108** is transmitted to the controller **109** for authorisation of the user for that location at that time.

In addition to authenticating the user **101** the biometric sensor **121** in the code entry module **103** in conjunction with the controller **107** can also check other access privileges of the user **101**. These access privileges can be contained in the database **105** which can be located either locally in the remote key fob, or in the receiver sub-system **117** as previously described. In one example, Tom Smith can firstly be authenticated as Tom Smith using the thumb press by Tom on the biometric sensor panel (not shown). After Tom's personal biometric identity is authenticated, the transmitter sub-system **116** can check if Tom Smith is in fact allowed to use the particular door secured by the device **111** on weekends. Thus the security screening offered by the described arrangement can range from simple authentication of the user's identity, to more comprehensive access privilege screening.

The incorporation of the biometric sensor **121** into the code entry module **103** in the form of a remote key fob also means that if the user **101** loses the remote key fob, the user need not be concerned that someone else can use it. Since the finder of the lost key fob will not be able to have his or her biometric signal authenticated by the biometric sensor **121** in the code entry module **103**, the lost key fob is useless to anyone apart from the rightful user **101**.

The transmitter sub-system **116** is preferably fabricated in the form of a single integrated circuit (IC) to reduce the possibility of an authorised person bypassing the biometric sensor **121** in the code entry module **103** and directly forcing the controller **107** to emit the rolling code access signal **108**.

FIG. **3** shows the method of operation of the remote control module (i.e. the sub-system **116**) of FIG. **2**. The method **200** commences with a testing step **201** in which the biometric sensor **121** in the code entry module **103** checks whether a biometric signal **102** is being received. If this is not the case, then the method **200** is directed in accordance with an NO arrow back to the step **201** in a loop. If, on the other hand, the biometric signal **102** has been received, then the method **200** is directed in accordance with a YES arrow to a step **202**. The step **202** compares the received biometric signal **102** with information in the biometric signature database **105** in order to ensure that the biometric signal received **102** is that of the rightful user **101** of the sub-system **116**.

A subsequent testing step **203** checks whether the comparison in the step **202** yields the desired authentication. If the biometric signature matching is authenticated, then the process **200** is directed in accordance with a YES arrow to a step **204**. The authentication of the biometric signature matching produces an accessibility attribute for the biometric signal **102** in question. The accessibility attribute establishes whether and under which conditions access to the controlled item **111** should be granted to a user. Thus, for example, the accessibility attribute may comprise one or more of an access attribute (granting unconditional access), a duress attribute (granting access but with activation of an alert tone to advise authorities of the duress situation), an alert attribute (sounding a chime indicating that an unauthorised, but not necessarily hostile, person is seeking access, and a telemetry attribute, which represents a communication channel for communicating state information for the transmitter sub-system to the receiver sub-system such as a "low battery" condition. The step **204** enables the user **101** to select a control option by providing one or more additional signals (not shown) to the controller **107**. Thus for example the control option could enable the user **101** to access one of a number of secure doors after his or her identity has been authenticated in the step **203**. In the subsequent step **205** the controller **107** sends the appropriate access signal **108** to the controller **109**. The process **200** is then directed in accordance with an arrow **206** back to the step **201**.

Thus for example the sub-system **116** can be provided with a single biometric sensor **121** in the code entry module **103** which enables the user **101** to select one of four door entry control signals by means of separate buttons on the controller **107** (not shown). This would enable the user **101**, after authentication by the biometric sensor **121** in the code entry module **103** and the controller **107** to obtain access to any one of the aforementioned for secure doors.

Returning to the testing step **203**, if the signature comparison indicates that the biometric signal **102** is not authentic, and has thus not been received from the proper user, then the process **200** is directed in accordance with a NO arrow back to the step **201**. In an alternate arrangement, the NO arrow from the step **203** could lead to a disabling step which would disable further operation of the sub-system **116**, either immediately upon receipt of the incorrect biometric signal **102**, or after a number of attempts to provide the correct biometric signal **102**.

FIG. **4** shows the method of operation of the control sub-system **117** of FIG. **2**. The method **300** commences with

a testing step **301** which continuously checks whether the access signal **108** has been received from **107**. The step **301** is performed by the controller **109**. As long as the access signal **108** is not received the process **300** is directed in accordance with a NO arrow in a looping manner back to the step **301**. When the access signal **108** is received, the process **300** is directed from the step **301** by means of a YES arrow to a step **302**. In the step **302**, the controller **109** compares the rolling code received by means of the access signal **108** with a reference code in the database **115**. A subsequent testing step **303** is performed by the controller **109**. In the step **303** if the code received on the access signal **108** is successfully matched against the reference code in the database **115** then the process **300** is directed in accordance with a YES arrow to a step **304**.

In the step **304** the controller **109** sends the control signal **110** to the controlled item **111** (for example opening the secured door). The process **300** is then directed from the step **304** as depicted by an arrow **305** back to the step **301**. Returning to the testing step **303** if the code received on the access signal **108** is not successfully matched against the reference code in the database **115** by the controller **109** then the process **300** is directed from the step **303** in accordance with a NO arrow back to the step **301**.

As was described in regard to FIG. **3**, in an alternate arrangement, the process **300** could be directed, if the code match is negative, from the step **303** to a disabling step which would disable the sub-system **117** if the incorrect code where received once or a number of times.

FIG. **5** shows incorporation of a protocol converter into the arrangement of FIG. **2**. In the arrangement of FIG. **2** the receiver **118** in the controller **109** is able to directly receive and process the rolling code in the access signal **108** in a manner as to provide, as depicted by the arrow **120**, the necessary information to the controller **109**. FIG. **5** shows how an existing controller depicted by a reference numeral **109'** that uses Wiegand input signalling can be used in the disclosed arrangement when alarm systems are upgraded. FIG. **5** shows how the incoming access signal **108** is received by a receiver **118'** as is the case in FIG. **2**. In FIG. **5** however the receiver **118'** provides, as depicted by an arrow **503**, the received rolling code from the access signal **108** to a rolling code/Wiegand protocol converter **501**. The converter **501** converts, as depicted by an arrow **504**, the incoming rolling code **503** to a form that can be used by the controller **109'** that is designed to handle Wiegand protocol incoming signals. Therefore, the converted incoming signal **504** is in the Wiegand format.

The converter **501** uses a microprocessor-based arrangement running software code to process the incoming rolling code information **503** and decode this information **503** to clear text form. The converter **501** converts this clear text to a Wiegand variable bit-length data stream. In FIG. **2**, the receiver **118** performs the conversion of the incoming rolling code access signal **108** to clear text which enables the controller **109** to identify the serial number of the originating key fob sub-system **116** to enable the access rights of the user to be verified.

Further to the Wiegand conversion arrangement, the protocol converter **501** approach can be adapted to convert between the incoming rolling code **503** (or any other appropriate secure code) to any other convenient protocol used by the controller **169'**.

The advantage of the rolling code/Wiegand converter **501** is that security system upgrades can be made without replacing Wiegand compatible controller **109'**. Accordingly, existing systems as are described in FIG. **1** can be upgraded by replacing the code entry module **403** and the transmission path **404**, leaving the other components of the system **400** (i.e., the controller **405**, the code database **407**, and the controlled item **409**, together with existing wiring **408** and **406**), largely intact. Minor modifications might however be necessary. When upgrading systems in this manner, the sub-system **116** can either be used in a remote fob configuration, or can be placed in a secure housing on an external door jamb.

From a practical perspective, incorporating the protocol converter **501** into an existing controller **109'** would require direct wiring of the converter **501** into the housing of the secure controller **109'**.

FIG. **6** shows another process **700** of operation of the remote access system. The process **700** commences with a step **701** that determines if a biometric signal has been received by the biometric sensor **121** in the code entry module in FIG. **2**. If not, then the process **700** follows a NO arrow back to the step **701**. If however a biometric signal has been received, then the process **700** follows a YES arrow to a step **702** that determines if the user ID database **105** in FIG. **2** is empty. This would be the case, for example, if the code entry module is new and has never been used, or if the user **101** has erased all the information in the database **105**.

If the database **105** is empty, then the process **700** is directed by an arrow **703** to **706** in FIG. **8** which depicts a process **800** dealing with the enrollment or the administration function for loading relevant signatures into the database **105**. If on the other hand the database **105** is not empty, then the process **700** is directed to a step **704** that determines if the biometric signal that has been received is an administrator's biometric signal.

The disclosed remote entry system can accommodate at least three classes of user, namely administrators, (ordinary) users, and duress users. The administrators have the ability to amend data stored, for example, in the database **105**, while the ordinary users do not have this capability. The first user of the code entry module **103**, whether this is the user who purchases the module, or the user who programs the module **103** after all data has been erased from the database **105**, is automatically categorised as an administrator. This first administrator can direct the system **100** to either accept further administrators, or alternately to only accept further ordinary users.

Although the present description refers to "Users", in fact it is "fingers" which are the operative entities in system operation when the biometric sensor **121** (see FIG. **2**) is a fingerprint sensor. In this event, a single user can enroll two or more of his or her own fingers as separate administrators or (ordinary) users of the system, by storing corresponding fingerprints for corresponding fingers in the database **105** via the enrollment process **800** (see FIG. **8**).

Some class overlap is possible. Thus a stored signature can belong to an administrator in the duress class.

The first administrator can provide control information to the code entry module by providing a succession of finger presses to the biometric sensor **121**, providing that these successive presses are of the appropriate duration, the appropriate quantity, and are input within a predetermined time. In one arrangement, the control information is encoded by either or both (a) the number of finger presses and (b) the relative duration of the finger presses. If the successive finger presses are provided within this predetermined time, then the controller **107** accepts the presses as potential control information and checks the input information against a stored set of legal control signals.

One example of a legal control signal can be expressed as follows:

"Enroll an ordinary user"→dit, dit, dit, dah where "dit" is a finger press of one second's duration (provided by the user **101** in response to the feedback provided by the Amber LED as described below), and "dah" is a finger press of two second's duration.

In the event that a legitimate sequence of finger presses are not delivered within the predetermined time, then the presses are considered not to be control information and merely to be presses intended to provide access to the controlled item **111**. Legitimate control sequences are defined in Read Only Memory (ROM) in the controller **107**.

The code entry module **103** has feedback signalling mechanisms **122**, implemented for example by a number of LEDs, and **124**, implemented by an audio transducer. The LEDs **122** and the audio transducer **124** are used by the controller to signal the state of the code entry module **103** to the user **101**, and to direct the administration process. Thus, in one example, three LEDs, being Red, Amber and Green are provided.

When the Amber LED is flashing, it means "Press the sensor". When the Amber LED is steady ON, it means "Maintain finger pressure". When the Amber LED is OFF, it means "Remove finger pressure". When the system enters the enrollment state (depicted by the process **800** in FIG. **8**), then the audio transducer **124** emits the "begin enrollment" signal (dit dit dit dit) and the Red LED flashes. Enrollment of a normal user (according to the step **807** in FIG. **8**) is signaled by the OK audio signal (dit dit) and a single blink of the Green LED.

Returning to the step **704**, if the step determines that the biometric signal received is an administrator's signal, then the process **700** is directed by a YES arrow to **706** in FIG. **8** as depicted by the arrow **703**. If on the other hand, the step **704** indicates that the received biometric signal does not belong to an administrator then the process **700** is directed by a NO arrow to **707** in FIG. **7**.

FIG. **7** shows the access process **600** by which a biometric signal **102** (see FIG. **2**) is processed in order to provide access to the controlled item **111**, or to take other action. Entering the process at **707** from FIG. **6**, the process **600** proceeds to a step **602** that compares the received biometric signature to signatures stored in the database **105**. A following step **603** determines if the received signal falls into the "duress" category. Signatures in this category indicate that the user **101** is in a coercive situation where, for example, an armed criminal is forcing the user **101** to access the secure facility (such as a bank door). If the step **603** determines that the signature is in the duress class, then a following step **604** prepares a "duress" bit for incorporation into the code access signal **108**. The aforementioned duress bit is an access attribute of the biometric signal **102**. Thereafter the process **600** proceeds to a step **605**.

Modules used in the code entry module for producing the rolling code enable a number of user defined bits to be inserted into the access signal **108**, and these bits can be used to effect desired control functions in the receiver sub-system **117**. The disclosed system **100** utilises four such user bits, namely (a) to indicate that the user belongs to the duress category, (b) to indicate a "battery low" condition, or other desired system state or "telemetry" variable, for the code entry module **103**, (c) to indicate that the biometric signal represents a legitimate user in which case the secure access to the controlled item **111** is to be granted, or (d) to indicate that the biometric signal is unknown, in which case the controller **109** in the receiver sub-system **117** sounds an alert tone using a bell (not shown) or the like.

Returning to FIG. **7**, if the step **603** determines that the biometric signal is not in the duress class, then the process **600** proceeds according to a NO arrow to the step **605**. The step **605** determines if the code entry module **103** has a low battery condition, in which event the process **600** proceeds according to a YES arrow to a step **606** that prepares a telemetry bit for insertion into the access signal **108**. The aforementioned telemetry bit is an access attribute of the biometric signal **102**. Thereafter, the process proceeds to a step **607**.

If the step **605** determines that telemetry signalling is not required, then the process **600** proceeds according to a NO arrow to the step **607**. The step **607** checks the biometric signal against the signatures in the database **105**. If the received biometric signal matches a legitimate signature in the database **105**, then the process is directed to a step **608** that prepares an "access" bit for insertion into the access signal **108**. This access bit directs the controller **109** in the receiver sub-system **117** to provide access to the controlled item **111**. The aforementioned access bit is an access attribute of the biometric signal **102**. The process **600** then proceeds to a step **610**.

If the step **607** determines that the biometric input signal does not match any legitimate signatures in the database **105**, then the process **600** proceeds according to a NO arrow to a step **609** that prepares an "alert" bit for insertion into the access signal **108**. The aforementioned alert bit is an access attribute of the biometric signal **102**. This alert bit directs the controller **109** (a) not to provide access to the controlled item **111**, and (b) to provide an alert tone, like ringing a chime or a bell (not shown), to alert personnel in the vicinity of the receiver sub-system **117** that an unauthorised user is attempting to gain access to the controlled item **111**. The alert bit can also cause a camera mounted near the controlled item **111** to photograph the unauthorised user for later identification of that person. The camera can be activated if the person attempting to gain access is unauthorised, and also if the person attempting to gain access is authorised but uses a duress signature.

An optional additional step (not shown) can prepare an identification field for insertion into the access signal **108**. This sends, to the receiver sub-system **117**, ID information that the receiver sub-system can use to construct an audit trail listing which users, having signatures in the database **105**, have been provided with access to the controlled item **111**.

The process **600** is then directed to the step **610** which inserts the various user defined bits into the access signal **108** and sends the signal **108** to the receiver sub-system **117**. Thereafter, the process **600** is directed by an arrow **611** to **705** in FIG. **6**.

FIG. **8** shows a process **800** for implementing various enrollment procedures. The process **800** commences at **706** from FIG. **6** after which a step **801** determines if the biometric signal is a first administrators input (which is the case if the database **105** is empty). If this is the case, then the process **800** is directed to a step **802** that stores the administrator's signature in the database **105**. From a terminology perspective, this first administrator, or rather the first administrator's first finger (in the event that the biometric sensor **121** in FIG. **2** is a fingerprint sensor), is referred to as the "superfinger". Further administrator's fingers are referred to as admin-fingers, and ordinary users fingers are referred to merely as "fingers". The reason that someone would enroll more than one of their own fingers into the system is to

ensure that even in the event that one of their enrolled fingers is injured, the person can still operate the system using another enrolled finger.

It is noted that the step **802**, as well as the steps **805**, **807** and **809** involve sequences of finger presses on the biometric sensor **121** in conjunction with feedback signals from the LEDs **122** and/or the audio speaker **124**. The process **800** then proceeds to a step **810** that determines if further enrollment procedures are required. If this is the case, then the process **800** proceeds by a YES arrow back to the step **801**. If no further enrollment procedures are required, then the process **800** proceeds by a NO arrow to **705** in FIG. **6**.

Returning to the step **801**, if the biometric signal is not a first administrator's signal, then the process **800** proceeds by a NO arrow to a step **803**. The step **803** determines if a further administrator signature is to be stored. It is noted that all signatures stored in the database are tagged as belonging to one or more of the classes of administrator, ordinary user, and duress users. If a further administrator signature is to be stored, then the process **800** proceeds by a YES arrow to the step **802** that stores the biometric signal as a further administrator's signature.

If a further administrator's signature is not required, then the process **800** proceeds according to a NO arrow to a step **804** that determines if a duress signature is to be stored. If this is the case then the process **800** follows a YES arrow to a step **805** that stores a duress signature. The process **800** then proceeds to the step **810**. If however the step **804** determines that a duress signature is not required, then the process **800** proceeds by a NO arrow to s step **806**.

The step **806** determines if a further simple signature (i.e. belonging to an ordinary user) is to be stored. If a further simple signature is to be stored, then the process **800** proceeds by a YES arrow to the step **807** that stores the biometric signal as a further ordinary signature.

If a further simple signature is not required, then the process **800** proceeds according to a NO arrow to a step **808** that determines if any or all signatures are to be erased from the database **105**. If this is the case then the process **800** follows a YES arrow to a step **809** that erases the desired signatures. The process **800** then proceeds to the step **810**. If however the step **804** determines that no signatures are to be erased, then the process **800** proceeds by a NO arrow to the step **810**.

FIG. **9** shows another enrollment process relating to the example of FIG. **6**. The process **900** commences at **706** from FIG. **6** after which a step **901** determines if the received biometric signal comes from the first administrator. If this is the case, then the process **900** proceeds according to a YES arrow to a step **902**. The step **902** emits an "Enrollment" tone and flashes the green LED once only. Thereafter, a step **905** reads the incoming biometric signal which is provided by the user as directed by the Amber LED. When the Amber LED flashes continuously, this directs the user to "Apply Finger". When the Amber LED is in a steady illuminated state, this directs the user to "Maintain Finger Pressure". Finally, when the amber LED is off, this directs the user to "Remove Finger".

Returning to the step **901**, if the incoming biometric signal does not belong to the first administrator, then the process **900** proceeds according to a NO arrow to a step **903**. The step **903** emits an "Enrollment" tone, and flashes the Red LED in an on-going fashion. Thereafter; the process **900** proceeds according to an arrow **904** to the step **905**.

Following the step **905**, a step **906** determines whether the incoming biometric signal is legible. If this is not the case, then the process **900** proceeds according to a NO arrow to a step **907**. The step **907** emits a "Rejection" tone, after which the process **900** is directed, according to an arrow **908** to **705** in FIG. **6**. Returning to the step **906**, if the incoming biometric signal is legible, then the process **900** follows a YES arrow to a step **909**. The step **909** determines whether the finger press exceeds a predetermined time. If this is not the case, then the process **900** follows a NO arrow to a step **910** which stores the biometric signal, which in the present case is a fingerprint signature. Thereafter the process **900** follows an arrow **911** to **705** in FIG. **6**.

Returning to the step **909** if the finger press does exceed the predetermined period, then the process follows a YES arrow to a step **912**. The step **912** erases relevant signatures depending upon the attributes of the incoming biometric signal. Thus, for example, if the incoming biometric signal belongs to an ordinary user, then the ordinary user's signature in the database **105** is erased by the step **912**. If, on the other hand, the incoming biometric signal belongs to the first administrator, then all the signatures in the database **105** are erased. Administrators who are not the first administrator can be granted either the same powers as the first administrator in regard to erasure of signatures, or can be granted the same powers as ordinary user in this respect.

Once the step **912** has completed erasure of the relevant signatures, then the process **900** follows an arrow **913** to **705** in FIG. **6**.

FIG. **10** is a schematic block diagram of the system in FIG. **2**. The disclosed secure access methods are preferably practiced using a computer system arrangement **100'**, such as that shown in FIG. **10** wherein the processes of FIGS. **3-4**, and **6-9** may be implemented as software, such as application program modules executing within the computer system **100'**. In particular, the method steps for providing secure access are effected by instructions in the software that are carried out under direction of the respective processor modules **107** and **109** in the transmitter and receiver sub-systems **116** and **117**. The instructions may be formed as one or more code modules, each for performing one or more particular tasks. The software may also be divided into two separate parts, in which a first part performs the provision of secure access methods and a second part manages a user interface between the first part and the user. The software may be stored in a computer readable medium, including the storage devices described below, for example. The software is loaded into the transmitter and receiver sub-systems **116** and **117** from the computer readable medium, and then executed under direction of the respective processor modules **107** and **109**. A computer readable medium having such software or computer program recorded on it is a computer program product. The use of the computer program product in the computer preferably effects an advantageous apparatus for provision of secure access.

The following description is directed primarily to the transmitter sub-system **116**, however the description applies in general to the operation of the receiver sub-system **117**. The computer system **100'** is formed, having regard to the transmitter sub-system **116**, by the controller module **107**, input devices such as the bio sensor **121**, output devices including the LED display **122** and the audio device **124**. A communication interface/transceiver **1008** is used by the controller module **107** for communicating to and from a communications network **1020**. Although FIG. **2** shows the transmitter sub-system **116** communicating with the receiver sub-system **117** using a direct wireless link for the access signal **108**, this link used by the access signal **108** can be effected over the network **1020** forming a tandem link comprising **108-1020-108'**. The aforementioned communi-

cations capability can be used to effect communications between the transmitter sub-system **116** and the receiver sub-system **117** either directly or via the Internet, and other network systems, such as a Local Area Network (LAN) or a Wide Area Network (WAN).

The controller module **107** typically includes at least one processor unit **1005**, and a memory unit **1006**, for example formed from semiconductor random access memory (RAM) and read only memory (ROM). The controller module **107** also includes an number of input/output (I/O) interfaces including an audio-video interface **1007** that couples to the LED display **122** and audio speaker **124**, an I/O interface **1013** for the bio-sensor **121**, and the interface **1008** for communications. The components **1007**, **1008**, **1005**, **1013** and **1006** the controller module **107** typically communicate via an interconnected bus **1004** and in a manner which results in a conventional mode of operation of the controller **107** known to those in the relevant art.

Typically, the application program modules for the transmitter sub-system **116** are resident in the memory **1006** iROM, and are read and controlled in their execution by the processor **1005**. Intermediate storage of the program and any data fetched from the bio sensor **121** and the network **1020** may be accomplished using the RAM in the semiconductor memory **1006**. In some instances, the application program modules may be supplied to the user encoded into the ROM in the memory **1006**. Still further, the software modules can also be loaded into the transmitter sub-system **116** from other computer readable media, say over the network **1020**. The term "computer readable medium" as used herein refers to any storage or transmission medium that participates in providing instructions and/or data to the transmitter sub-system **116** for execution and/or processing. Examples of storage media include floppy disks, magnetic tape, CD-ROM, a hard disk drive, a ROM or integrated circuit, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the transmitter sub-system **116**. Examples of transmission media include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

INDUSTRIAL APPLICABILITY

It is apparent from the above that the arrangements described are applicable to the security industry.

The foregoing describes only some embodiments of the present invention, and modifications and/or changes can be made thereto without departing from the scope and spirit of the invention, the embodiments being illustrative and not restrictive.

The system **100** can also be used to provide authorised access to lighting systems, building control devices, exterior or remote devices such as air compressors and so on. The concept of "secure access" is thus extendible beyond mere access to restricted physical areas.

The invention claimed is:

1. A system for providing secure access to a controlled item, the system comprising:

a memory comprising a database of biometric signatures;

a transmitter sub-system comprising:

a biometric sensor configured to receive a biometric signal;

a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute; and

a receiver sub-system comprising:

a receiver sub-system controller configured to:

receive the transmitted secure access signal; and

provide conditional access to the controlled item dependent upon said information;

wherein the transmitter sub-system controller is further configured to:

receive a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

map said series into an instruction; and

populate the data base according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

2. The system according to claim **1**, wherein the transmitter sub-system controller is further configured to:

provide a signal for directing input of the series of entries of the biometric signal;

incorporate into the secure access signal an identification field identifying the biometric signal if the signal matches a member of the database; and

construct an audit trail of biometric signals provided to the biometric sensor in order to access the controlled item.

3. The system according to claim **1**, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class, the accessibility attribute comprising:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures and said member belongs to the duress class; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

4. The system according to claim **1**, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration, and/or the database of biometric signatures is located in at least one of the transmitter sub-system and the receiver sub-system.

5. The system according to claim **1**, wherein said conditional access comprises one of:

provision of access to the controlled item if the accessibility attribute comprises an access attribute:

provision of access to the controlled item and sounding of an alert if the accessibility attribute comprises a duress attribute; and

denial of access to the controlled item and sounding of an alert if the accessibility attribute comprises an alert attribute.

6. The system as claimed in claim **1**, wherein the biometric sensor is further configured to authenticate the identity of a user;

wherein the transmitter is further configured to transmit information capable of granting access to the controlled item using a secure wireless signal dependent upon a request from the user and the authentication of the user identity; and

the system further comprising a control panel configured to receive the information and provide the secure access requested.

7. The system according to claim **6**, wherein the control panel includes a converter configured to receive the secure wireless signal and output the information, and/or the biometric sensor is configured to authenticate the identity of the user by comparing a biometric input from the user with a biometric signature for the user in a biometric database, and/or the biometric sensor, the biometric database, and the transmitter are located in a remote fob.

8. The system according to claim **7**, wherein the secure wireless signal comprises an RF carrier and a rolling code, and the converter converts the rolling code to the Wiegand protocol.

9. The system according to claim **1**, wherein:

the transmitter sub-system and the receiver sub-system are collocated in the electronic computing device.

10. A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:

a biometric sensor configured to receiving a biometric signal;

a controller configured to match the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and

a transmitter configured to emit a secure access signal conveying said information dependent upon said accessibility attribute;

wherein the controller is further configured to:

receive a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

map said series into an instruction; and

populate the database according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

11. A method for providing secure access to a controlled item in a system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor configured to receive a biometric signal, and a transmitter configured to emit a secure access signal capable of granting access to the controlled item, and a receiver sub-system comprising a receiver sub-system controller configured to receive the transmitted secure access signal, and provide conditional access to the controlled item dependent upon information in said secure access signal, the method comprising:

populating the database of biometric signatures by:

receiving a series of entries of the biometric signal;

determining at least one of the number of said entries and a duration of each said entry;

mapping said series into an instruction; and

populating the database according to the instruction;

receiving the biometric signal;

matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;

emitting a secure access signal conveying information dependent upon said accessibility attribute; and

providing conditional access to the controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

12. The method according to claim **11**, wherein populating the database of biometric signatures further comprises enrolling a biometric signature into the database of biometric signatures, and wherein enrolling the biometric signature into the database comprises:

receiving a biometric signal; and

enrolling the biometric signal as an administrator signature in response to the database of biometric signatures being empty.

13. The method according to claim **12**, wherein enrolling the biometric signature further comprises receiving another biometric signal to confirm the enrolling of the biometric signal as an administrator signature, and wherein enrolling the biometric signature is dependent upon generation of a feedback signal adapted to direct provision of at least one of the biometric signal and the other biometric signal.

14. A non-transitory computer readable storage medium storing a computer program comprising instructions, which when executed by processors causes the processors to:

receive a series of entries of a biometric signal;

determine at least one of a number of said entries and a duration of each of said entries;

map said series into an instruction;

populate a database of biometric signatures according to the instruction;

receive the biometric signal;

match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;

emit a secure access signal conveying information dependent upon said accessibility attribute; and

provide conditional access to a controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

15. A system for providing secure access to a controlled item, the system comprising:

a memory comprising a database of biometric signatures;

a transmitter sub-system comprising:

a biometric sensor capable of receiving a biometric signal;

a transmitter sub-system controller capable of matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

a transmitter capable of emitting a secure access signal conveying information dependent upon said accessibility attribute; and

a receiver sub-system comprising:

a receiver sub-system controller capable of:

receiving the transmitted secure access signal; and

providing conditional access to the controlled item dependent upon said information;

wherein the transmitter sub-system controller is further capable of:

receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

mapping said series into an instruction; and

populating the data base according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

16. A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:

a biometric sensor capable of receiving a biometric signal;

a controller capable of matching the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and

a transmitter capable of emitting a secure access signal conveying said information dependent upon said accessibility attribute;

wherein the controller is further capable of:

receiving a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

mapping said series into an instruction; and

populating the database according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

17. A method for providing secure access to a controlled item in a system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor capable of receiving a biometric signal, and a transmitter capable of emitting a secure access signal capable of granting access to the controlled item, and a receiver sub-system comprising a receiver sub-system controller capable of receiving the transmitted secure access signal, and providing conditional access to the controlled item dependent upon information in said secure access signal, the method comprising:

populating the database of biometric signatures by:

receiving a series of entries of the biometric signal;

determining at least one of the number of said entries and a duration of each said entry;

mapping said series into an instruction; and

populating the database according to the instruction;

receiving the biometric signal;

matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;

emitting a secure access signal conveying information dependent upon said accessibility attribute; and

providing conditional access to the controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

* * * * *

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATIONS

Case Number: 24-1278, 24-1354

Short Case Caption: CPC Patent Technologies Pty Ltd. v. Apple Inc.

Instructions: When computing a word, line, or page count, you may exclude any items listed as exempted under Fed. R. App. P. 5(c), Fed. R. App. P. 21(d), Fed. R. App. P. 27(d)(2), Fed. R. App. P. 32(f), or Fed. Cir. R. 32(b)(2).

The foregoing filing complies with the relevant type-volume limitation of the Federal Rules of Appellate Procedure and Federal Circuit Rules because it meets one of the following:

☑ the filing has been prepared using a proportionally-spaced typeface and includes 5,954 words.

☐ the filing has been prepared using a monospaced typeface and includes _____ lines of text.

☐ the filing contains _____ pages / _____ words / _____ lines of text, which does not exceed the maximum authorized by this court's order (ECF No. _____).

Date: 04/22/2024

Signature: /s/ George Summerfield

Name: George Summerfield

Save for Filing